AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXVI

1944

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

AMERICAN

JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXVI, Number 1
JANUARY, 1944

THE JOHNS HOPKINS PRESS
BALTIMORE, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS will appear four times yearly.

The subscription price of the JOURNAL for the current volume is $7.50 (foreign postage 50 cents); single numbers $2.00.

A few complete sets of the JOURNAL remain on sale.

Papers intended for publication in the JOURNAL may be sent to any of the Editors.

Editorial communications may be sent to Professor F. D. MURNAGHAN at The Johns Hopkins University.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE, MARYLAND, U. S. A.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

AN EXTENSION OF GALOIS THEORY TO NON-NORMAL AND NON-SEPARABLE FIELDS.* [1]

By N. JACOBSON.

As is well known, modern Galois theory is a theory of the automorphisms of an arbitrary field P. Its principal result is the establishment of a $(1-1)$ correspondence between the finite groups $\mathfrak{g}$ of automorphisms in P and the subfields $\Phi_{\mathfrak{g}}$ over which P is finite, separable and normal, such that 1) $\mathfrak{g}_1 \geq \mathfrak{g}_2$ if and only if $\Phi_{\mathfrak{g}_1} \leq \Phi_{\mathfrak{g}_2}$ and 2) $\mathfrak{g}_2$ is invariant in $\mathfrak{g}_1$ if and only if $\Phi_{\mathfrak{g}_2}$ is normal over $\Phi_{\mathfrak{g}_1}$. A second type of Galois theory has been given by the author in a previous paper.[2] It associates the subfields Φ of a field P of characteristic p over which P has the form $\Phi(x_1, \cdots, x_m)$ where $x_i^p = \xi_i$ in Φ with certain algebras of derivations in P. In seeking an extension of these theories we have been led to a study of the *self-representations* of P, i. e. the representations of P by matrices with elements in this field.[3] One is led to seek an extension along these lines by the following two remarks. First, if S is an automorphism, then $\alpha \to \alpha^S$ is a self-representation by 1-dimensional matrices and second, if D is a derivation, then

$$\alpha \to \begin{pmatrix} \alpha & \alpha D \\ 0 & \alpha \end{pmatrix}$$

is a representation by 2-rowed matrices.

Now by our definition of a self-representation any isomorphism of P into a subfield is a self-representation. It is therefore desirable to restrict the

* Received July 12, 1943.

[1] Presented to the Society, September 11, 1943.

[2] "Abstract derivation and Lie algebras," *Transactions of the American Mathematical Society*, vol. 43 (1937), p. 220.

[3] A Galois theory of separable extensions which makes use of the concept of self-representation has been announced recently by L. Kaloujnine, "Sur la théorie de Galois des corps non galoisiens séparables," *Comptes Rendus de l'Académie des Sciences*, vol. 214 (1942), pp. 597-599. (Abstracted in *Mathematical Reviews*, vol. 4 (1943), p. 130). It appears that Kaloujnine's results are special cases of those obtained here. See **12**. It should be mentioned also that Galois theory for separable extensions based on the classical theory for separable normal extensions had been developed previously. See Krasner, M. "Sur la théorie de la ramification des ideaux des corps non-galoisiens de nombres algebriques," *Thèse*, Paris, 1938. The present theory (and apparently that of Kaloujnine) is independent of the classical theory.

class of self-representations in such a way that any self-representation in this class having rank one (one-rowed) is an automorphism of P. This has been done by defining *non-singular* self-representations. There is a natural way to define the product of two self-representations: One substitutes for the elements of the matrices of one representation the matrices representing these elements in the second representation. This, of course, is a generalization of the product of isomorphisms.

With any self-representation—or more exactly, with any class of similar self-representations—we may associate a double P-module $\mathfrak{R}$ having the property that its right dimensionality $(\mathfrak{R}:\mathrm{P}_r) = m < \infty$. If, in addition, $(\mathfrak{R}:\mathrm{P}_l) = m$, then $\mathfrak{R}$ is said to be non-singular. Modules of this type correspond to non-singular self-representations. One may also define a product for double modules corresponding to the product of self-representations.

Now with each self-representation we may associate a composite (ring) of the field P with itself. This consists of the ring of transformations in P generated by the scalar multiplications $x \to \alpha x$ and $x \to x\alpha$. These composites may also be defined abstractly: A system (K, S, T) is a *composite* of P with itself if K is a ring and S and T are isomorphisms between P and subfields P^S and P^T of K such that 1) $K = \mathrm{P}^S\mathrm{P}^T$, 2) K is commutative, 3) $1^S = 1^T$, 4) $(K:\mathrm{P}^T) < \infty$. If (K', S', T') is a second composite and the mapping $\Sigma\alpha^S\beta^T \to \Sigma\alpha'^{S}\beta^{T'}$ is a homomorphism, then (K, S, T) is a *cover* of (K', S', T') $((K, S, T) \geqq (K', S', T'))$. If this mapping is an isomorphism, the two composites are equivalent. Throughout our discussion equivalent composites are identified. One may define non-singular composites and the product $(K, S, T) \times (L, U, V)$ of any two composites. A composite (K, S, T) is called a *Galois composite* if $(K, S, T) \geqq (K, S, T) \times (K, S, T)$, (K, S, T) $\geqq$ the identity composite (P^U, U, U) and $(K, S, T) = (K, T, S)$. Our main result is the establishment of a $(1-1)$ correspondence between the Galois composites Γ of P and the subfields Φ_Γ of P over which P is finite, such that $\Gamma_1 \geqq \Gamma_2$ if and only if $\Phi_{\Gamma_1} \leqq \Phi_{\Gamma_2}$.

Any composite may be decomposed in a certain sense into indecomposable composites (K_i, S_i, T_i). Conditions that (K, S, T) be a Galois composite may be given in terms of the components (K_i, S_i, T_i). If each K_i is a field, (K, S, T) is called *semi-simple*. In this case the condition that (K, S, T) be a Galois composite is that the components (K_i, S_i, T_i) form a hypergroup relative to the product $(K_i, S_i, T_i)(K_j, S_j, T_j)$ defined to be the set of components of the composite $(K_i, S_i, T_i) \times (K_j, S_j, T_j)$. Our fundamental correspondence between composites and subfields induces a $(1-1)$ correspondence between semi-simple Galois composites and subfields Φ over which

P is finite and separable. We investigate also the fields Φ over which P is normal. Combining our results for normal and separable fields we obtain a $(1-1)$ correspondence between the semi-simple composites whose hypergroups are groups and the subfields Φ over which P is finite, separable and normal. Finally, it is easy to obtain the connection between these composites and finite groups of automorphisms and this gives the classical theorem.

Our results could have been formulated in terms of self-representations but this seems to be unnatural except in the case where P has a primitive element over Φ. In a later paper we hope to investigate in greater detail the theory for subfields Φ over which P is purely inseparable.

1. Self-representations of fields. If P is an arbitrary field, we define a *self-representation* of P as an isomorphism between P and a field of m-rowed matrices with elements in P such that $1 \rightarrow 1$ the identity matrix. The integer m is the *rank* of the representation. If $E: \alpha \rightarrow \alpha^E$ in P_m is a self-representation, we define E_{ij} as the transformation sending α into the element in the i-th row and j-th column of α^E.[4] Thus $\alpha^E = (\alpha E_{ij})$ and the E_{ij} satisfy the following conditions:

$$(1) \qquad (\alpha + \beta)E_{ij} = \alpha E_{ij} + \beta E_{ij}, \qquad (\alpha\beta)E_{ij} = \Sigma_\lambda (\alpha E_{i\lambda})(\beta E_{\lambda j}), \\ 1E_{ij} = \delta_{ij}$$

Conversely any m^2 transformations E_{ij} in P that satisfy (1) determine a self-representation $\alpha \rightarrow (\alpha E_{ij})$ of P.

We shall call γ a *fixed element* under E if γ^E is the diagonal matrix $\{\gamma, \cdots, \gamma\}$. Hence γ is fixed if $\gamma E_{ii} = \gamma$ and $\gamma E_{ij} = 0$ for $i \neq j$. Evidently the set of fixed elements is a subfield of P.

We shall recall now some of the important concepts from general representation theory. Two self-representations E and F are *similar* if there exists a fixed non-singular matrix $S = (\sigma_{ij})$ such that $\alpha^F = S^{-1}\alpha^E S$ for all α. Similar representations evidently have the same fixed elements. A representation is *reducible* if it is similar to a representation F in which $F_{ij} = 0$ for $i > r > 0$ and $j \leq r$. In this case the correspondences $\alpha \rightarrow (\alpha F_{kl})$ $k, l = 1, \cdots, r$ and $\alpha \rightarrow (\alpha F_{pq})$, $p, q = r + 1, \cdots, m$ are self-representations. The first of these is a *subrepresentation* and the second a *difference representation* of E. If besides $F_{ij} = 0$ for $i > r$ and $j \leq r$ we have $F_{ij} = 0$ for $i \leq r$ and $j > r$, then E is *decomposable* into the *components* $\alpha \rightarrow (\alpha F_{kl})$, $\alpha \rightarrow (\alpha F_{pq})$. In a similar manner decomposability into more than two components may be de-

---

[4] P_m denotes the ring of $m \times m$ matrices with elements in P.

fined. We shall write $E = E_1 + E_2 + \cdots + E_s$ when E is decomposable into the components E_i. If $E = E_1 + \cdots + E_s$ where the E_i are irreducible, E is said to be *completely reducible.* If an element γ of P is a fixed element relative to E, it is fixed under any subrepresentation and under any difference representation of E.

2. Double P-modules. We shall now give a module formulation of the representation problem. We define a *double* P-*module*[5] as a commutative group $\mathfrak{R}$ which is both a right P-module and a left P-module such that

1. $$1x = x = x1.$$
2. $$(\alpha x)\beta = \alpha(x\beta).$$

Thus if we denote the endomorphism $x \to \alpha x$ by α_l and the endomorphism $x \to x\alpha$ by α_r then $\alpha_l\beta_r = \beta_r\alpha_l$ for all α, β in P. We denote the field of endomorphisms $\alpha_l(\alpha_r)$ by $P_l(P_r)$. For our purposes it suffices to consider only double P-modules that satisfy the following condition

3. $$(\mathfrak{R} : P_r) = m < \infty.$$

Hence from now on we use the term "double P-module" for "double P-module satisfying condition 3."

Let $x_1, \cdots, x_m$ be a basis for $\mathfrak{R}$ over P_r. Then $\alpha x_i = \Sigma x_j \alpha_{ji}$ and it is readily verified that the correspondence $\alpha \to (\alpha_{ij})$ is a self-representation E of P. The rank of E is m. Conversely if E is any self-representation, then we let $\mathfrak{R}$ be a right P-module such that $(\mathfrak{R} : P_r) = m$. If $x_1, \cdots, x_m$ is a basis for $\mathfrak{R}$, we write $x = \Sigma x_i \xi_i$ and define $\alpha x = \Sigma x_j \eta_j$ where $\eta_j = \Sigma(\alpha E_{ij})\xi_i$. Then it is readily verified that $\mathfrak{R}$ is a double P-module and $\alpha x_i = \Sigma x_j(\alpha E_{ji})$. Thus any self-representation is obtained from some double P-module in the manner indicated. If $y_1, \cdots, y_m$, $y_i = \Sigma x_j \sigma_{ji}$ is a second basis over P_r of the double P-module $\mathfrak{R}$, then $\alpha y_i = \Sigma y_j(\alpha F_{ji})$ and $(\alpha F_{ij}) = \alpha^F = S^{-1}\alpha^E S$ where $S = (\sigma_{ij})$. Hence the different right bases for $\mathfrak{R}$ correspond to the different self-representations similar to E.

It is clear that an element γ of P is a fixed element under E if and only if $\gamma_l = \gamma_r$.

If $\mathfrak{S}$ is a submodule of $\mathfrak{R}$, αy and $y\alpha \in \mathfrak{S}$ for any y in $\mathfrak{S}$ and any α in P.

---

[5] Cf. E. Noether, "Hyperkomplexe Grössen und Darstellungstheorie," *Mathematische Zeitschrift*, vol. 30 (1929), p. 669; v. d. Waerden, *Moderne Algebra*, vol. 2, p. 131; or Jacobson, *The Theory of Rings*, New York, 1943, p. 95 (referred to hereafter as *R*).

We may choose a basis $y_1, \cdots, y_m$ of $\mathfrak{R}$ over P_r such that $y_1, \cdots, y_r$ is a basis for $\mathfrak{S}$ over P_r. Then $\alpha y_k = \Sigma y_l \alpha_{lk}$, $k, l = 1, \cdots, r$. Hence E is reducible and the representation F determined by $\mathfrak{S}$ is a subrepresentation of E. Also we have $\alpha y_p \equiv \Sigma y_q \alpha_{qp} \pmod{\mathfrak{S}}$ for $p, q = r + 1, \cdots, m$. Hence the representation G determined by the difference P-module $\mathfrak{R} - \mathfrak{S}$ is a difference representation of E. In a similar manner we see that the condition that E be decomposable is that $\mathfrak{R}$ be a direct sum of submodules $\neq 0$ and the condition that E be completely reducible is that $\mathfrak{R}$ be a completely reducible double module.

3. Composites. If $\mathfrak{R}$ is a double P-module, the set of transformations that are finite sums of products $\alpha_l \beta_r$ is a ring $P_l P_r = P_r P_l$. The elements of $P_l P_r$ belong to $\mathfrak{L}$ the algebra of linear transformations of $\mathfrak{R}$ over P_r. Now we recall that the scalar multiplications in the algebra $\mathfrak{L}$ are the mappings $A \to A\alpha_r = \alpha_r A$ and that the dimensionality of $\mathfrak{L}$ over P_r is m^2. Since $P_l P_r \geq P_r$, $P_l P_r$ is a subalgebra of $\mathfrak{L}$. Hence $(P_l P_r : P_r) = q \leq m^2$.

We now define a *composite* of a field with itself as a system (K, S, T) consisting of a ring K and two isomorphisms S and T between P and subfields P^S and P^T of K such that the following conditions hold:

1. $K = P^S P^T$
2. $\alpha^S \beta^T = \beta^T \alpha^S$ for all α, β
3. $1^S = 1^T$
4. $(K : P^T) < \infty$.

Evidently by 1. and 2., K is a commutative ring and by 1. and 3. $1^S = 1^T$ is an identity element 1 in K. We have seen that any double P-module $\mathfrak{R}$ determines a composite $(P_l P_r, L, R)$ where L denotes the isomorphism $\alpha \to \alpha_l$ and R denotes the isomorphism $\alpha \to \alpha_r$.

In all of our work we shall identify composites (K, S, T) and (K', S', T') that are *equivalent* in the sense that there exists an isomorphism $k \to k'$ between K and K' such that $(\alpha^S)' = \alpha^{S'}$, $(\alpha^T)' = \alpha^{T'}$. The composite (K, S, T) will be called a *cover* of (K', S', T') $((K, S, T) \geq (K', S', T'))$ if there exists a homomorphism $k \to k'$ between K and K' such that $(\alpha^S)' = \alpha^{S'}$, $(\alpha^T)' = \alpha^{T'}$. Since $K = P^S P^T$, it is clear that if such a homomorphism exists, it is unique. In fact, it may be characterized by the fact that it maps $\Sigma \alpha^S \beta^T$ into $\Sigma \alpha^{S'} \beta^{T'}$. This, of course, implies that the mapping $\Sigma \alpha^S \beta^T \to \Sigma \alpha^{S'} \beta^{T'}$ is single-valued. Thus if $\Sigma \alpha^S \beta^T = 0$, then $\Sigma \alpha^{S'} \beta^{T'} = 0$. Conversely if the latter condition holds, the mapping $\Sigma \alpha^S \beta^T \to \Sigma \alpha^{S'} \beta^{T'}$ is a homomorphism and hence $(K, S, T) \geq (K', S', T')$. The condition that (K, S, T) and (K', S', T') be equivalent

is that $\Sigma\alpha^S\beta^T = 0$ holds in K if and only if $\Sigma\alpha^{S'}\beta^{T'} = 0$ holds in K'. Thus $(K, S, T) = (K', S', T')$ if and only if $(K, S, T) \geqq (K', S', T')$ and $(K', S', T') \geqq (K, S, T)$. If $(K, S, T) \geqq (K', S', T')$ and $(K', S', T') \geqq (K'', S'', T'')$, then $(K, S, T) \geqq (K'', S'', T'')$. By the fundamental theorem of homomorphisms of rings any composite covered by (K, S, T) is equivalent to a composite $(K - B, \bar{S}, \bar{T})$ where B is an ideal in K and $\bar{S}$ and $\bar{T}$ are obtained from S and T by applying the natural homomorphism that maps the element k of K into its coset $\bar{k} = k + B$.

Any composite is equivalent to a composite determined by a double P-module. For we may take $\mathfrak{R}$ to be K and define $\alpha x = \alpha^S x = x\alpha^S$ and $x\alpha = \alpha^T x = x\alpha^T$ for any x in $\mathfrak{R}$ and any α in P. Then $(\mathfrak{R} : \mathrm{P}_r) = (K : \mathrm{P}^T)$ is finite. It is readily seen that the composite $(\mathfrak{R}, L, R)$ of $\mathfrak{R}$ is equivalent to (K, S, T).

If $\mathfrak{S}$ is a submodule or a difference module of a double P-module $\mathfrak{R}$, then the correspondence between $\Sigma\alpha_l\beta_r$ in $\mathfrak{R}$ and $\Sigma\alpha_l\beta_r$ in $\mathfrak{S}$ is clearly a homomorphism. Thus the composite $(\mathrm{P}_l\mathrm{P}_r, L, R; \mathfrak{R})$ associated with $\mathfrak{R}$ is a cover of the composite $(\mathrm{P}_l\mathrm{P}_r, L, R; \mathfrak{S})$. If $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$ then if $\Sigma\alpha_l\beta_r = 0$ in both $\mathfrak{R}_1$ and $\mathfrak{R}_2$, $\Sigma\alpha_l\beta_r = 0$ in $\mathfrak{R}$. It follows that $(\mathrm{P}_l\mathrm{P}_r, L, R; \mathfrak{R})$ is a *least common cover* of the composites $(\mathrm{P}_l\mathrm{P}_r, L, R; \mathfrak{R}_i)$, $i = 1, 2$, in the sense that any cover of the latter two composites is a cover of $(\mathrm{P}_l\mathrm{P}_r, L, R; \mathfrak{R})$. We may also define the least common cover $(K, S, T) + (L, U, V)$ for any two composites (K, S, T) and (L, U, V) abstractly: For let $K \oplus L$ be the direct sum of the rings K and L. The elements of $K \oplus L$ are uniquely representable in the form, $k + l$, $k \epsilon K$ and $l \epsilon L$ and $(k + l)(k' + l') = kk' + ll'$. We set $\alpha^X = \alpha^S + \alpha^U$ and $\alpha^Y = \alpha^T + \alpha^V$. Then the set of elements $\alpha^X(\alpha^Y)$ is a field $\mathrm{P}^X(\mathrm{P}^Y)$ isomorphic to P. If $k_1, \cdots, k_q$ is a basis for K over P^T and $l_1, \cdots, l_r$ is a basis for L over P^V, the elements $k_1, \cdots, k_q; l_1, \cdots, l_r$ form a basis for $K \oplus L$ over P^Y. Thus $((K + L) : \mathrm{P}^Y)$ is finite. Hence if $M = \mathrm{P}^X\mathrm{P}^Y$, we may conclude also that $(M : \mathrm{P}^Y)$ is finite. Thus (M, X, Y) is a composite of P with itself. Since $\Sigma\alpha^X\beta^Y = \Sigma(\alpha^S + \alpha^U)(\beta^T + \beta^V) = \Sigma(\alpha^S\beta^T + \alpha^U\beta^V) = 0$ if and only if $\Sigma\alpha^S\beta^T = 0$ and $\Sigma\alpha^U\beta^V = 0$, (M, X, Y) is a least common cover of (K, S, T) and (L, U, V). The least common cover is uniquely determined in the sense of equivalence. In a similar fashion we may define a least common cover for any finite number of composites.

We have seen that the fixed elements of a self-representation E are the elements γ such that $\gamma_l = \gamma_r$ in the double P-module associated with E. Evidently these elements are determined by the composite $(\mathrm{P}_l\mathrm{P}_r, L, R)$. Accordingly we define an element γ of P to be a *fixed element* of a composite $\Gamma = (K, S, T)$ if $\gamma^S = \gamma^T$. These elements form a subfield Φ_Γ of P.

4. The relations space of a composite. Let $\Gamma = (K, S, T)$ be a composite of P with itself and suppose that $(K : P^T) = q$. Since $K = P^S P^T$, there exists a basis for K over P^T consisting of elements $\alpha_1^S, \cdots, \alpha_q^S$ in P^S. For any α in P we may write

$$\alpha^S = \alpha_1^S \mu_1(\alpha)^T + \cdots + \alpha_q^S \mu_q(\alpha)^T. \tag{2}$$

Since this expression is unique, the mapping $M_i : \alpha \to \mu_i(\alpha)$ is single-valued. Since $(\alpha + \beta)^S = \alpha^S + \beta^S$, $\mu_i(\alpha + \beta)^T = \mu_i(\alpha)^T + \mu_i(\beta)^T$ and hence

$$(\alpha + \beta) M_i = \alpha M_i + \beta M_i. \tag{3}$$

If γ is a fixed element under Γ, $(\alpha\gamma)^S = \alpha^S \gamma^S = \alpha^S \gamma^T$. Hence

$$(\alpha\gamma) M_i = (\alpha M_i)\gamma. \tag{4}$$

Now suppose that

$$\alpha_i^S \alpha_j^S = \Sigma \alpha_k^S \epsilon_{kij}^T. \tag{5}$$

Then

$$\alpha^S \beta^S = (\Sigma \alpha_i^S \mu_i(\alpha)^T)(\Sigma \alpha_j^S \mu_j(\beta)^T) = \Sigma \alpha_k^S \epsilon_{kij}^T \mu_i(\alpha)^T \mu_j(\beta)^T.$$

On the other hand, $\alpha^S \beta^S = (\alpha\beta)^S = \Sigma \alpha_i^S \mu_i(\alpha\beta)^T$ so that

$$(\alpha\beta) M_i = \Sigma_{\lambda,\mu} \epsilon_{i\lambda\mu} (\alpha M_\lambda)(\beta M_\mu). \tag{6}$$

These equations may be written in a more useful form as follows: If β is any element of P, we let $\bar{\beta}$ denote the multiplication $\alpha \to \alpha\beta = \beta\alpha$. With this notation equation (4) becomes

$$\bar{\gamma} M_i = M_i \bar{\gamma} \tag{4'}$$

and (6) becomes

$$\bar{\beta} M_i = \Sigma M_\lambda \bar{\zeta}_{\lambda i} \tag{6'}$$

where $\zeta_{\lambda i} = \Sigma_\mu \epsilon_{i\lambda\mu} (\beta M_\mu)$. Equation (3) states that M_i is an endomorphism of the additive group of P. Of course, the multiplications $\bar{\beta}$ are also endomorphisms. Hence this is true for any transformation of the form $\Sigma M_i \bar{\rho}_i$, ρ_i in P.

We suppose now that $\beta_1, \cdots, \beta_q$ is a second set of elements such that

$\beta_1{}^S, \cdots, \beta_q{}^S$ is a basis for K over P^T. Then $\beta_i{}^S = \Sigma\alpha_j{}^S\rho_{ji}{}^T$ where $(\rho_{ij}) = R$ is a non-singular matrix. If $R^{-1} = (\sigma_{ij})$ and

$$\alpha^S = \beta_1{}^S\nu_1(\alpha)^T + \cdots + \beta_q{}^S\nu_q(\alpha)^T$$

then $\mu_i(\alpha)^T = \Sigma\rho_{ij}{}^T\nu_j(\alpha)^T$ and $\nu_i(\alpha)^T = \Sigma\sigma_{ij}{}^T\mu_j(\alpha)^T$. Thus

$$(7) \qquad M_i = \Sigma N_j\bar{\rho}_{ij} \quad \text{and} \quad N_i = \Sigma M_j\bar{\sigma}_{ij}.$$

Hence the totality $\mathfrak{A}$ of endomorphisms (of the additive group of P) of the form $\Sigma M_i\bar{\rho}_i$ is independent of the choice of the basis. It is clear also that any two equivalent composites determine the same sets $\mathfrak{A}$. The set $\mathfrak{A}$ is evidently closed under multiplication on the right by the multiplications $\bar{\rho}$. By (6′) $\mathfrak{A}$ is also closed under multiplication by $\bar{\rho}$ on the left. We assert now that the M_i are right linearly independent relative to the $\bar{\rho}$. For by (2), $\alpha_i M_j = \delta_{ij}$. Hence $\alpha_i\Sigma M_j\bar{\rho}_j = \rho_i$ and so if $\Sigma M_j\bar{\rho}_j = 0$, $\rho_i = 0$ and $\bar{\rho}_i = 0$. We shall call $\mathfrak{A}$ the *relations space* of the composite (K, S, T) and we shall denote the set of multiplications $\bar{\rho}$ by $\bar{\mathrm{P}}$. We have therefore proved the following

THEOREM 1. *If $\mathfrak{A}$ is the relations space of the composite (K, S, T) and $\bar{\mathrm{P}}$ is the set of multiplications, then $\mathfrak{A}\bar{\mathrm{P}} \leq \mathfrak{A}$ and $\bar{\mathrm{P}}\mathfrak{A} \leq \mathfrak{A}$. The right dimensionality $(\mathfrak{A} : \bar{\mathrm{P}})_r = (K : \mathrm{P}^T)$.*[6]

5. Conditions for covering composites. If $\mathfrak{R}$ is a two-sided P-module we have defined the composite of $\mathfrak{R}$ as $(\mathrm{P}_l\mathrm{P}_r, L, R)$ where L is the correspondence $\alpha \to \alpha_l$ and R is the correspondence $\alpha \to \alpha_r$. Now let $x_1, \cdots, x_m$ be a basis for $\mathfrak{R}$ over P_r and set $\alpha x_i = \Sigma x_j(\alpha E_{ij})$. As we have seen the correspondence $\alpha \to \alpha^E = (\alpha E_{ij})$ is a self-representation. By the well-known isomorphism between linear transformations and matrices, we may substitute for α_l the matrix α^E and for α_r the matrix $\alpha^D = \{\alpha, \cdots, \alpha\}$ and obtain in this way a new composite equivalent to $(\mathrm{P}_l\mathrm{P}_r, L, R)$. We denote this composite as $(\mathrm{P}^E\mathrm{P}^D, E, D)$ where E is the mapping $\alpha \to \alpha^E$ and D is the mapping $\alpha \to \alpha^D$.

Consider now the transformations E_{ij}. By (1) E_{ij} is an endomorphism of the additive group of P and the set of E_{ij} satisfy the following conditions:

---

[6] Using (5) and (6′) one can show that the self-representation determined by the basis M_i of the double P-module $\mathfrak{A}$ is E' the transposed representation of the self-representation E determined by the basis $\alpha_1 S, \cdots, \alpha_q S$ of K. See a forthcoming paper of the author's entitled "Construction of central simple associative algebras."

$$\bar{\gamma} E_{ij} = E_{ij} \bar{\gamma} \tag{8}$$

if $\gamma \epsilon \Phi$ the field of fixed elements and

$$\bar{\beta} E_{ij} = \Sigma E_{i\lambda}(\overline{\beta E_{\lambda j}}). \tag{9}$$

As in the preceding section we determine the transformations M_i by choosing elements $\alpha_1, \cdots, \alpha_q$ such that each $\alpha_l = \alpha_{1l}\mu_1(\alpha)_r + \cdots \alpha_{ql}\mu_q(\alpha)_r$ uniquely. Then $\alpha^E = \alpha_1{}^E \mu_1(\alpha)^D + \cdots + \alpha_q{}^E \mu_q(\alpha)^D$ and

$$\alpha E_{ij} = \mu_1(\alpha)(\alpha_1 E_{ij}) + \cdots + \mu_q(\alpha)(\alpha_q E_{ij}).$$

Thus

$$E_{ij} = M_1(\overline{\alpha_1 E_{ij}}) + M_2(\overline{\alpha_2 E_{ij}}) + \cdots + M_q(\overline{\alpha_q E_{ij}}) \tag{10}$$

is in the relations space $\mathfrak{A}$ of our composite. It follows that the set of endomorphisms of the form $\Sigma E_{ij}\bar{\rho}_{ij}$, where the $\bar{\rho}$ are arbitrary multiplications, is a subspace $\mathfrak{B}$ of $\mathfrak{A}$ regarded relative to $\bar{\mathrm{P}}$ on the right. We assert that $\mathfrak{B} = \mathfrak{A}$. For otherwise there exist $p < q$ endomorphisms $N_1, \cdots, N_p$ in $\mathfrak{A}$ such that

$$E_{ij} = N_1 \bar{\sigma}_{ij1} + \cdots + N_p \bar{\sigma}_{ijp},$$

or $\alpha E_{ij} = (\alpha N_1)\sigma_{ij1} + \cdots + (\alpha N_p)\sigma_{ijp}$. Thus each matrix α^E is a linear combination of the p matrices $\sigma_k = (\sigma_{ijk})$, $k = 1, \cdots, p$, with coefficients $\alpha N_k{}^D$ and this contradicts the fact that $\alpha_1{}^E, \cdots, \alpha_q{}^E$ are linearly independent over P^D. This proves

THEOREM 2. *If E_{ij} are the E's determined by a self-representation E, then the set of endomorphisms $\Sigma E_{ij}\bar{\rho}_{ij}$ is the complete relations space $\mathfrak{A}$ of the composite associated with E.*

Suppose now that $\Gamma = (K, S, T)$ is a cover of the composite $\Gamma' = (K', S', T')$. We determine the M_i for K by equation (2). Then

$$\alpha^{S'} = \alpha_1{}^{S'}\mu_1(\alpha)^{T'} + \cdots + \alpha_q{}^{S'}\mu_q(\alpha)^{T'}$$

and every element of K' is a linear combination of the $\alpha_i{}^{S'}$ with coefficients in $\mathrm{P}^{T'}$. Now let $\beta_1, \cdots, \beta_p$, $p \leq q$ be elements of P such that the $\beta_k{}^{S'}$ form a basis over $\mathrm{P}^{T'}$ of K'. Then we have $\alpha_i{}^{S'} = \Sigma \beta_k{}^{S'} \rho_{ki}{}^{T'}$. Hence

$$\alpha^{S'} = \beta_1{}^{S'}\nu_1(\alpha)^{T'} + \cdots + \beta_p{}^{S'}\nu_p(\alpha)^{T'}$$

where $\nu_k(\alpha)^{T'} = \Sigma \mu_i(\alpha)^{T'}\rho_{ki}{}^{T'}$. The mappings $N_k\colon \alpha \to \nu_k(\alpha)$ form a basis

for the relations space $\mathfrak{A}(\Gamma')$ of Γ' and we have shown that $N_k = \Sigma M_{i}\bar{\rho}_{ki}$. Thus $\mathfrak{A}(\Gamma') \leq \mathfrak{A}(\Gamma)$.

Now suppose conversely that $\mathfrak{A}(\Gamma') \leq \mathfrak{A}(\Gamma)$. Let $\mathfrak{R}$ and $\mathfrak{S}$ be double P-modules that have composites equivalent to (K, S, T) and (K', S', T') respectively. Let E be a self-representation determined by $\mathfrak{R}$ and F one determined by $\mathfrak{S}$. Since $\mathfrak{A}(\Gamma') \leq \mathfrak{A}(\Gamma)$ it follows from Theorem 2 that there exist elements $\rho_{ij,kl}$ such that $F_{kl} = \Sigma E_{ij}\bar{\rho}_{ji,kl}$ for all k and l. These equations may be written in the form

$$\alpha F_{kl} = \mathrm{tr}(\alpha^E \rho_{kl}) \tag{11}$$

where ρ_{kl} is the matrix $(\rho_{ij,kl})$. Now suppose that we have a relation of the form $\Sigma\alpha^E\beta^D = 0$ where $\beta^D = \{\beta, \cdot\cdot\cdot, \beta\}$. Then it follows readily from (11) that $\Sigma\alpha^F\beta^D = 0$. Thus (K, S, T) is a cover for (K', S', T'). This completes the proof of the following important

THEOREM 3. *A necessary and sufficient condition that the composite $\Gamma \geq \Gamma'$ is that the relations space $\mathfrak{A}(\Gamma) \geq \mathfrak{A}(\Gamma')$.*

This implies

THEOREM 4. *A necessary and sufficient condition that $\Gamma = \Gamma'$ is that $\mathfrak{A}(\Gamma) = \mathfrak{A}(\Gamma')$.*

6. Non-singular composites. If (K, S, T) is a composite such that $(K : \mathrm{P}^S) < \infty$, it defines a new composite (K, T, S). It may happen that both $(K : \mathrm{P}^S)$ and $(K : \mathrm{P}^T)$ are finite but that these dimensionalities are not equal. For example let $K = \mathrm{P} = \Phi(t)$ the field of rational functions in one indeterminate over Φ. Let T be the identity and S the automorphism defined by $t^S = t^2$. Then the self-representation determined by K is the isomorphism $\alpha(t) \to \alpha(t^2)$ that maps P into a proper subfield. We may avoid this type of situation by restricting our attention to composites (K, S, T) that are *non-singular* in the sense that $(K : \mathrm{P}^S) = (K : \mathrm{P}^T)$. If (K, S, T) is non-singular, the composite (K, T, S) will be called the *inverse* of (K, S, T). If (K, S, T) is equivalent to (K, T, S) we shall call this composite *symmetric.*

Corresponding to the concept of non-singular composite, we define a double P-module $\mathfrak{R}$ to be *non-singular* if $(\mathfrak{R} : \mathrm{P}_l) = (\mathfrak{R} : \mathrm{P}_r)$. Suppose that $\mathfrak{R}$ has this property. We prove first the following

LEMMA. *There exists a set of elements $y_1, \cdot\cdot\cdot, y_m$ that constitute both a left and a right basis for $\mathfrak{R}$ over* P.

The element y_1 may be taken to be any element $\neq 0$ in $\mathfrak{R}$. Then $y_1\alpha \neq 0$ and $\alpha y_1 \neq 0$ for all $\alpha \neq 0$. Now suppose that $y_1, \cdots, y_r$ are elements of $\mathfrak{R}$ which are left linearly independent and right linearly independent over P. Then if $r < m = (\mathfrak{R} : \mathrm{P}_l) = (\mathfrak{R} : \mathrm{P}_r)$, there is an element y not of the form $\Sigma\alpha_i y_i$. If y does not have the form $\Sigma y_i\alpha'_i$ either, y may be taken to be the element y_{m+1}. Hence suppose that $y = \Sigma y_i\alpha'_i$. Similarly we choose an element z not of the form $\Sigma y_i\beta_i$ and we may suppose that $z = \Sigma\beta'_i y_i$. Now form $w = y + z$. Then if $w = \Sigma y_i\alpha_i$, $z = w - y = \Sigma y_i(\alpha_i - \alpha'_i)$ contrary to assumption. Similarly, w cannot be represented in the form $\Sigma\beta_i y_i$. Hence we may take $y_{m+1} = w$. This process leads to a basis of the required type.

The same method may be used to show that if $\mathfrak{S}$ is a non-singular submodule of $\mathfrak{R}$, there exists a two-sided basis for $\mathfrak{R}$ that includes a two-sided basis for $\mathfrak{S}$.

Now if $\mathfrak{R}$ is a non-singular double P-module, we shall define the inverse $\mathfrak{R}^{-1}$ of $\mathfrak{R}$ to be the module whose elements may be put in $(1-1)$ correspondence with the elements of $\mathfrak{R}$ in such a way that if $x \to x'$ in $\mathfrak{R}^{-1}$,

$$
\begin{aligned}
(x+y)' &= x' + y' \\
(\alpha x)' &= x'\alpha \\
(x\alpha)' &= \alpha x'.
\end{aligned}
\tag{12}
$$

Thus $\mathfrak{R}^{-1}$ is obtained from $\mathfrak{R}$ by interchanging the roles of P_l and P_r. If $x_1, \cdots, x_m$ is a left (right) basis for $\mathfrak{R}$, then $x'_1, \cdots, x'_m$ is a right (left) basis for $\mathfrak{R}^{-1}$. Let $y_1, \cdots, y_m$ be a two-sided basis for $\mathfrak{R}$ and $\alpha y_i = \Sigma y_j(\alpha E_{ji})$, $y_i\alpha = \Sigma(\alpha E^*_{ji})y_j$. Then we recall that the correspondence $\alpha \to \alpha^E = (\alpha E_{ij})$ is a self-representation determined by $\mathfrak{R}$.. In $\mathfrak{R}^{-1}$ we have $\alpha y'_i = \Sigma y'_j(\alpha E^*_{ji})$ and $y'_i\alpha = \Sigma(\alpha E_{ji})y'_j$. Thus $\alpha \to \alpha^{E^*} = (\alpha E^*_{ij})$ is the self-representation associated with $\mathfrak{R}^{-1}$. We note that

$$
\begin{aligned}
\alpha y_i &= \Sigma y_j(\alpha E_{ji}) = \Sigma(\alpha E_{ji}E^*_{kj})y_k \\
y_i\alpha &= \Sigma(\alpha E^*_{ji})y_j = \Sigma y_k(\alpha E^*_{ji}E_{kj}).
\end{aligned}
$$

Hence $\alpha\delta_{ik} = \Sigma\alpha E_{ji}E^*_{kj}$ and $\alpha\delta_{ik} = \Sigma\alpha E^*_{ji}E_{kj}$ or

$$
\Sigma E_{ji}E^*_{kj} = \delta_{ik}, \qquad \Sigma E^*_{ji}E_{kj} = \delta_{ik}. \tag{13}
$$

These equations may be written in a simpler form by introducing the ring $\mathfrak{E}_m$ of m-rowed matrices with elements in the ring $\mathfrak{E}$ of endomorphisms of the additive group of P. For we set $(E) = (E_{ij})$ and call this matrix in $\mathfrak{E}_m$ the matrix of the *self-representation*. If $(E^*) = (E^*_{ij})$ then (13) may be replaced by the single equation

$$(14) \qquad (E)'(E^*)' = 1 = (E^*)'(E)'$$

where the prime denotes the transposed matrix. The representation $\alpha \rightarrow (\alpha E^*_{ij})$ will be called the *inverse* E^{-1} *of the representation* E.

If (K, S, T) is a non-singular composite, we have seen that we may take K to be a double P-module by setting $\alpha x = \alpha^S x = x\alpha^S$ and $x\alpha = \alpha^T x = x\alpha^T$. The dimensionality $(\mathfrak{R} : \mathrm{P}_l) = (K : \mathrm{P}^S) = (K : \mathrm{P}^T) = (\mathfrak{R} : \mathrm{P}_r)$. Hence $\mathfrak{R}$ is non-singular and its inverse is $\mathfrak{R}^{-1} = (K, T, S)$ with P_l here $= \mathrm{P}^T$ and $\mathrm{P}_r = \mathrm{P}^S$. If we choose two-sided bases in these modules we obtain a pair of inverse self-representations of P.

If (K, S, T) and (L, U, V) are non-singular composites, their least common cover (M, X, Y) is also non-singular. For, let $\mathfrak{R}$ be a double P-module such that $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$ where the $\mathfrak{R}_i$ are non-singular submodules and $\mathfrak{R}_1$ has the composite (K, S, T) and $\mathfrak{R}_2$ has the composite (L, U, V). Then $(\mathfrak{R} : \mathrm{P}_l) = (\mathfrak{R}_1 : \mathrm{P}_l) + (\mathfrak{R}_2 : \mathrm{P}_l) = (\mathfrak{R}_1 : \mathrm{P}_r) + (\mathfrak{R}_2 : \mathrm{P}_r) = (\mathfrak{R} : \mathrm{P}_r)$ and so $\mathfrak{R}$ is non-singular. Thus (M, X, Y) is non-singular. Its inverse (M, Y, X) is evidently the least common cover of (K, T, S) and (L, V, U). It follows from this that if (K, S, T) is an arbitrary non-singular composite, then $(K, S, T) + (K, T, S)$ is a symmetric composite.

7. The product of self-representations. If E and F are two self-representations of rank m and r respectively, they determine a self-representation of rank mr obtained by substituting for the elements αE_{ij} of α^E the matrices $(\alpha E_{ij})^F$ that represent these elements under F. We shall call this representation the *product* $E \times F$ *of the representations* E and F. The product $E \times F$ is an associative one. Moreover if 1 denotes the identity self-representation $\alpha \rightarrow (\alpha)$ of one row, then $E \times 1 = E = 1 \times E$ for all E. Hence the set of self-representations forms a semi-group with an identity relative to our composition. If (E) is the matrix of E and (F) is the matrix of F, then the matrix (P) of $P = E \times F$ is the (right) direct product $(E) \times (F)$, i. e. $P_{(i-1)r+k,\,(j-1)r+l} = E_{ij}F_{kl}$.

We shall define next a product of double P-modules that corresponds to the product of self-representations. Let $\mathfrak{R}$ and $\mathfrak{S}$ be two double P-modules. We wish to construct a double P-module $\mathfrak{P}$ and a function xy of x in $\mathfrak{R}$ and of y in $\mathfrak{S}$ such that the following conditions obtain:

1. $\alpha(xy) = (\alpha x)y$
2. $(xy)\alpha = x(y\alpha)$
3. $(x\alpha)y = x(\alpha y)$
4. $x(y + y') = xy + xy'$

5. $(x+x')y = xy + x'y$
6. Any element of $\mathfrak{P}$ has the form Σxy for suitable x in $\mathfrak{R}$ and y in $\mathfrak{S}$.
7. $(\mathfrak{P}:\mathrm{P}_r) = (\mathfrak{R}:\mathrm{P}_r)(\mathfrak{S}:\mathrm{P}_r)$.

Let $x_1, \cdots, x_m$ be a right basis for $\mathfrak{R}$ and $\alpha x_i = \Sigma x_j(\alpha E_{ji})$ and let $y_1, \cdots, y_r$ be a right basis for $\mathfrak{S}$ and $\alpha y_k = \Sigma y_l(\alpha F_{lk})$. Then if $x = \Sigma x_i \xi_i$ and $y = \Sigma y_k \eta_k$ conditions 1.-5. imply that

$$xy = \Sigma x_j y_l (\xi_j F_{lk}) \eta_k. \tag{15}$$

By 6. every element of $\mathfrak{P}$ is a linear combination of the elements $x_i y_k$. Hence by 7. these elements form a right basis for $\mathfrak{P}$ over P. The procedure for defining $\mathfrak{P}$ and xy is now clear. We let $\mathfrak{P}$ be a right module of dimensionality mr over P and define xy by (15) where $x_i y_k = z_{(i-1)r+k}$ form a basis for $\mathfrak{P}$. Then 2., 3., 4., 5. and 6. are valid. Next we define α_l to be the linear transformation in $\mathfrak{P}$ over P_r that sends $x_i y_k$ into $\Sigma x_j y_l(\alpha E_{ji} F_{lk})$. We set $\alpha z = \alpha_l z$ and we observe that $\alpha(xy) = \Sigma x_\lambda y_\sigma(\alpha E_{\lambda j} F_{\sigma l})(\xi_j F_{lk})\eta_k$. We may now verify that 1. holds and hence $\mathfrak{P}$ is a double P-module and xy is a function satisfying our conditions.

If $x'_1, \cdots, x'_m$ and $y'_1, \cdots, y'_r$, respectively, form a second pair of right bases for $\mathfrak{R}$ and for $\mathfrak{S}$, $x = \Sigma x'_i \xi'_i$ and $y = \Sigma y'_k \eta'_k$. Hence $xy = \Sigma x'_j y'_l(\alpha F'_{lk})\eta'_k$. Thus all the xy are linear combinations of the elements $x'_i y'_k$ and so these elements form a second right basis for $\mathfrak{P}$. Now suppose that we construct a second space $\mathfrak{P}'$ and a second function xy which we shall denote as $[xy]$ by using the bases x'_i and y'_k in place of the x_i and the y_k. Then it is readily verified that the mapping $\Sigma x'_i y'_k \xi_{ik} \to \Sigma[x'_i y'_k]\xi_{ik}$ is an isomorphism between the double P-modules $\mathfrak{P}$ and $\mathfrak{P}'$. In this sense the module $\mathfrak{P}$ does not depend on the choice of the bases x_i and y_k. We shall therefore denote this module as $\mathfrak{R} \times \mathfrak{S}$ and shall call it the *product of the modules* $\mathfrak{R}$ *and* $\mathfrak{S}$.

By definition

$$\alpha(x_i y_k) = \Sigma x_j y_l(\alpha E_{ji} F_{lk}).$$

Hence the representation determined by the basis z_s, $z_{(i-1)r+k} = x_i y_k$ is the product $E \times F$. The independence of $\mathfrak{P} = \mathfrak{R} \times \mathfrak{S}$ of the bases of $\mathfrak{R}$ and $\mathfrak{S}$ may be stated as

THEOREM 5. *If E' and F' are self-representations similar respectively to E and F, then $E' \times F'$ is similar to $E \times F$.*

If $x'_1, \cdots, x'_p$ are right linearly independent in $\mathfrak{R}$ and $y'_1, \cdots, y'_q$ are right linearly independent in $\mathfrak{S}$ then the elements $x'_j y'_l$ are right linearly

independent in $\mathfrak{P}$. For we may supplement the x' and the y' to obtain bases $x'_1, \cdots, x'_m$; $y'_1, \cdots, y'_r$. Then we have seen that the elements $x'_i y'_k$ are linearly independent. Now suppose that the elements $x'_1, \cdots, x'_p$ form a right basis for a submodule $\mathfrak{R}'$ of $\mathfrak{R}$ and the elements $y'_1, \cdots, y'_q$ form a right basis for a submodule $\mathfrak{S}'$ of $\mathfrak{S}$. Then the elements $x'_j y'_l$ form a basis for a submodule $\mathfrak{P}'$ of $\mathfrak{P}$ and $\mathfrak{P}'$ is essentially the module $\mathfrak{R}' \times \mathfrak{S}'$. This proves

THEOREM 6. *If E' is a subrepresentation of E and F' is a subrepresentation of F, then $E' \times F'$ is a subrepresentation of $E \times F$.*

In a similar manner we may prove

THEOREM 7. *If E is decomposable into the components E_i and F is decomposable into the components F_j, then $E \times F$ is decomposable into the components $E_i \times F_j$.*

We suppose now that $\mathfrak{R}$ and $\mathfrak{S}$ are non-singular double P-modules and that the x_i and y_k are two-sided bases. Let the elements x'_i and y'_k form the corresponding two-sided bases for $\mathfrak{R}^{-1}$ and $\mathfrak{S}^{-1}$. If $\alpha x_i = \Sigma x_j(\alpha E_{ji})$, $\alpha x'_i = \Sigma x'_j(\alpha E^*_{ji})$ where the self-representation E^* thus determined is the inverse of E. Similarly $\alpha y_k = \Sigma y_l(\alpha F_{lk})$ and $\alpha y'_k = \Sigma y'_l(\alpha F^*_{lk})$ where F^* is the inverse of F. Now $x_i\alpha = \Sigma(\alpha E^*_{ji})x_j$ and $y_k\alpha = \Sigma(\alpha F^*_{lk})y_l$ and so $(x_i y_k)\alpha = \Sigma(\alpha F^*_{lk}E^*_{ji})x_j y_l$. Hence every element of $\mathfrak{R} \times \mathfrak{S}$ is a left linear combination of the elements $x_i y_k$. These form a basis. For if $\Sigma \mu_{ik} x_i y_k = 0$, $\Sigma x_j y_l \mu_{ik} E_{ji} F_{lk} = 0$ and hence $\Sigma \mu_{ik} E_{ji} F_{lk} = 0$ for all j and l. It follows that $\mu_{i'k'} = \Sigma_{l,j} \mu_{ik} E_{ji} F_{lk} F^*_{k'l} E^*_{i'j} = 0$. We have therefore proved that $\mathfrak{R} \times \mathfrak{S}$ is non-singular and that the elements $x_i y_k$ form a two-sided basis for this module. The elements $(x_i y_k)'$ form a two-sided basis for the inverse module and we have $\alpha(x_i y_k)' = \Sigma(x_j y_l)'(\alpha F^*_{lk}E^*_{ji})$. Our argument shows also that the elements $y'_k x'_i$ form a two-sided basis for $\mathfrak{S}^{-1} \times \mathfrak{R}^{-1}$ and we may verify that $\alpha y'_k x'_i = \Sigma y'_l x'_j(\alpha F^*_{lk}E^*_{ji})$. Hence the modules $(\mathfrak{R} \times \mathfrak{S})^{-1}$ and $\mathfrak{S}^{-1} \times \mathfrak{R}^{-1}$ are isomorphic.

8. The product of composites. It is easy to see from Theorems 2 and 4 that the composite determined by $\mathfrak{R} \times \mathfrak{S}$ depends only on the composite of $\mathfrak{R}$ and the composite of $\mathfrak{S}$. For the composite of $\mathfrak{R} \times \mathfrak{S}$ has as its relations space the smallest subspace over $\bar{\mathrm{P}}$ (on the right) containing all of the products MN where M is in the relations space of the composite of $\mathfrak{R}$ and N is in the relations space of the composite of $\mathfrak{S}$. Thus the composite of $\mathfrak{R} \times \mathfrak{S}$ may be regarded as the product of the composite of $\mathfrak{R}$ by the composite of $\mathfrak{S}$. It is of interest to give a direct definition of the product of composites. We shall

obtain such a definition by introducing a type of three-fold composite of P with itself. Aside from its use in the present connection, the concept of a three-fold composite will play an important role in the proof in **9** of one of the main results of the present theory.

We define first a *three-fold composite* of P with itself as a system (Δ, A, B, C) consisting of a ring Δ and the isomorphisms A, B, C of P into subfields P^A, P^B, P^C of Δ such that

1. $\Delta = \mathrm{P}^A\mathrm{P}^B\mathrm{P}^C$
2. Δ is commutative
3. $1^A = 1^B = 1^C$.

Evidently by 1. and 3., $1^A = 1^B = 1^C$ is the identity 1 of Δ.

Covers of three-fold composites are defined in the obvious way: (Δ, A, B, C) is a cover of (Δ', A', B', C') if there is a homomorphism $a \rightarrow a'$ between Δ and Δ' such that $(\alpha^A)' = \alpha^{A'}$, $(\alpha^B)' = \alpha^{B'}$, $(\alpha^C)' = \alpha^{C'}$. Equivalence is defined in a similar manner.

Now suppose that (K, S, T) and (L, U, V) are arbitrary (two-fold) composites. We wish to construct a three-fold composite (Δ, A, B, C) having the following properties:

4. $(\mathrm{P}^A\mathrm{P}^B, A, B)$ is equivalent to (K, S, T) and $(\mathrm{P}^B\mathrm{P}^C, B, C)$ is equivalent to (L, U, V).
5. $(\Delta : \mathrm{P}^C) = (K : \mathrm{P}^T)(L : \mathrm{P}^V)$.

We shall show first that any two three-fold composites having these properties are equivalent. For this purpose let $\alpha_1, \cdots, \alpha_q$ be a set of elements of P such that $\alpha_1^S, \cdots, \alpha_q^S$ form a basis for K over P^T and let $\beta_1, \cdots, \beta_{q'}$ be elements such that $\beta_1^U, \cdots, \beta_{q'}^U$ form a basis for L over P^V. As before, we determine the endomorphisms $\alpha \rightarrow \mu_i(\alpha) \equiv \alpha M_i$ and $\alpha \rightarrow \nu_j(\alpha) \equiv \alpha N_j$ by writing

$$\alpha^S = \alpha_1^S \mu_1(\alpha)^T + \cdots + \alpha_q^S \mu_q(\alpha)^T$$
$$\alpha^U = \beta_1^U \nu_1(\alpha)^V + \cdots + \beta_{q'}^T \nu_{q'}(\alpha)^V.$$

Suppose also that

$$\alpha_i^S \alpha_{i'}^S = \Sigma \alpha_\lambda^S \epsilon_{\lambda i i'}^T, \qquad \beta_j^U \beta_{j'}^U = \Sigma \beta_\nu^U \eta_{\nu j j'}^V.$$

In Δ we have $\alpha^A = \Sigma \alpha_i^A \mu_i(\alpha)^B$, $\alpha^B = \Sigma \beta_j^B \nu_j(\alpha)^C$ and $\alpha_i^A \alpha_{i'}^A = \Sigma \alpha_\lambda^A \epsilon_{\lambda i i'}^B$, $\beta_j^B \beta_{j'}^B = \Sigma \beta_\nu^B \eta_{\nu j j'}^C$. Hence

$$(16) \quad \alpha_i^A \alpha_{i'}^A = \Sigma \alpha_\lambda^A \epsilon_{\lambda i i'}^B = \Sigma \alpha_\lambda^A \beta_j^B \nu_j(\epsilon_{\lambda i i'})^C, \quad \beta_j^B \beta_{j'}^B = \Sigma \beta_\nu^B \eta_{\nu j j'}^C.$$

Let $\bar{\Delta}$ denote the totality of elements of the form $\Sigma \alpha_i^A \beta_j^B \zeta_{ij}^C$. By (16), $\bar{\Delta}$ is a subring of Δ. Since

$$(17) \qquad \alpha^A = \Sigma\alpha_i{}^A\mu_i(\alpha)^B = \Sigma\alpha_i{}^A\beta_j{}^B\nu_j(\mu_i(\alpha))^C,$$

$P^A \leq \bar{\Delta}$. Hence 1 and $P^C \leqq \bar{\Delta}$. Moreover, $\beta_j{}^B = (\alpha_i{}^A)^{-1}(\alpha_i{}^A\beta_j{}^B) \epsilon \bar{\Delta}$ and so each $\alpha^B = \Sigma\beta_j{}^B\nu_j(\alpha)^C$ is in $\bar{\Delta}$. Thus $\bar{\Delta} = \Delta$ and every element of Δ is a linear combination with coefficients in P^C of the qq' elements $\alpha_i{}^A\beta_j{}^B$. Hence by 5. the elements $\alpha_i{}^A\beta_j{}^B$ form a basis for Δ over P^C.

Now suppose that (Δ', A', B', C') is a second three-fold composite having the properties 4. and 5. Then the mapping $\Sigma\alpha_i{}^A\beta_j{}^B\zeta_{ij}{}^C \to \Sigma\alpha_i{}^{A'}\beta_j{}^{B'}\zeta_{ij}{}^{C'}$ is clearly $(1-1)$ and by (16), it is an isomorphism. It is evident from the above considerations that this isomorphism maps α^A into $\alpha^{A'}$, α^B into $\alpha^{B'}$ and α^C into $\alpha^{C'}$.

We now construct the composite (Δ, A, B, C). Suppose that the elements $\alpha_i{}^S$ and $\beta_j{}^U$ have been chosen in the way indicated above. We shall suppose in addition that $\alpha_1{}^S = 1^S$ and $\beta_1{}^U = 1^U$. Now let P^C be a field isomorphic to P under the isomorphism $\alpha \to \alpha^C$ and let Δ be the algebra over P^C with the basis $\alpha_i{}^A\beta_j{}^B$ and the multiplication table

$$(18) \qquad (\alpha_i{}^A\beta_j{}^B)(\alpha_{i'}{}^A\beta_{j'}{}^B) = \Sigma\alpha_\lambda{}^A\beta_\mu{}^B\eta_{\mu k\nu}{}^C\eta_{\nu jj'}{}^C\nu_k(\epsilon_{\lambda ii'})^C.$$

We shall show that Δ is associative and that Δ determines a composite satisfying our conditions. We note first that $\alpha_1{}^A\beta_1{}^B$ acts as the identity 1 of Δ. The elements $\beta_j{}^B \equiv \alpha_1{}^A\beta_j{}^B$ satisfy the multiplication table $\beta_j{}^B\beta_{j'}{}^B = \Sigma\beta_\nu{}^B\eta_{\nu jj'}{}^C$ and these elements are linearly independent over P^C. It follows that the set of elements $\alpha^B = \Sigma\beta_j{}^B\nu_j(\alpha)^C$ is a subfield P^B of Δ isomorphic under the correspondence $\alpha^B \to \alpha$ to P. The totality of elements $\Sigma\beta_j{}^B\rho_j{}^C$ where the ρ_j are arbitrary defines a composite (P^BP^C, B, C) equivalent to (L, U, V). We note next that if we set $\alpha_i{}^A \equiv \alpha_i{}^A\beta_1{}^B$ the product of this element with $\beta_j{}^B$ (in either order) is the element $\alpha_i{}^A\beta_j{}^B$ of Δ. The elements $\alpha_i{}^A$ satisfy the relations

$$\alpha_i{}^A\alpha_{i'}{}^A = \Sigma\alpha_\lambda{}^A\beta_\mu{}^B\nu_\mu(\epsilon_{\lambda ii'})^C = \Sigma\alpha_\lambda{}^A\epsilon_{\lambda ii'}{}^B$$

and these elements are linearly independent over P^B. If we make use of equations for the ν_k analogous to (6), we may prove that $(\alpha_i{}^A\rho^B)(\alpha_{i'}{}^A\sigma^B) = \Sigma\alpha_\lambda{}^A\epsilon_{\lambda ii'}{}^B\rho^B\sigma^B$. It follows that the totality of elements of the form $\Sigma\alpha_i{}^A\rho_i{}^B$ is a ring isomorphic to K. The set of elements $\alpha^A = \Sigma\alpha_i{}^A\mu_i(\alpha)^B$ is a field P^A isomorphic under the correspondence $\alpha^A \to \alpha$ to P and the set of elements $\Sigma\alpha_i{}^A\rho_i{}^B$ determines a composite (P^AP^B, A, B) equivalent to (K, S, T). Now the elements of Δ may be written in one and only one way in the form $\Sigma\alpha_i{}^Al_i$ where $l_i \epsilon P^BP^C$. We may prove that $(\alpha_i{}^Al)(\alpha_{i'}{}^Am) = \Sigma\alpha_\lambda{}^A(\epsilon_{\lambda ii'}{}^Blm)$ and this implies that Δ is associative. Since Δ is generated by P^A, P^B and

$\mathrm{P}^C \equiv 1\mathrm{P}^C$, Δ is commutative. Conditions 4. and 5. are evidently satisfied. Hence (Δ, A, B, C) is the required three-fold composite.

We now define the *product of the composites* $(K, S, T) \times (L, U, V)$ as the composite $(\mathrm{P}^A\mathrm{P}^C, A, C)$ determined from the three-fold composite (Δ, A, B, C) that we have constructed. This product is uniquely determined. It can be seen that if (K, S, T) is a cover of (K', S', T') and (L, U, V) is a cover of (L', U', V'), then the three-fold composite (Δ, A, B, C) is a cover of the three-fold composite (Δ', A', B', C') constructed from (K', S', T') and (L', U', V'). It follows that $(K, S, T) \times (L, U, V)$ is a cover of $(K', S', T') \times (L', U', V')$. If (K, S, T) and (L, U, V) are non-singular, the three-fold composite (Δ, C, B, A) has the same relation to (L, V, U) and (K, T, S) as (Δ, A, B, C) has to (K, S, T) and (L, U, V). Hence $(L, V, U) \times (K, T, S) = (\mathrm{P}^A\mathrm{P}^C, C, A)$ and the latter is the inverse of $(\mathrm{P}^A\mathrm{P}^C, A, C)$. It is not difficult to give a direct proof of the associative law for multiplication of composites. For this purpose it is necessary to construct of four-fold composite (E, A, B, C, D) such that $(\mathrm{P}^A\mathrm{P}^B\mathrm{P}^C, A, B, C)$ is equivalent to (Δ, A, B, C) and $(\mathrm{P}^B\mathrm{P}^C\mathrm{P}^D, B, C, D)$ is equivalent to the composite $(\Delta_1, A_1, B_1, C_1)$ determined by (L, U, V) and (M, X, Y). We shall not carry through this proof but instead we shall obtain the associative law indirectly by determining the relations space of the product of the composites (K, S, T) and (L, U, V).

Let $\delta_1^A, \cdots, \delta_r^A$ be a basis for $\mathrm{P}^A\mathrm{P}^C$ over P^C and suppose that

$$\alpha^A = \delta_1^A\pi_1(\alpha)^C + \cdots + \delta_r^A\pi_r(\alpha)^C. \tag{19}$$

Then the endomorphisms $\alpha \to \pi_k(\alpha) \equiv \alpha P_k$ form a basis over $\overline{\mathrm{P}}$ of the relations space of the composite $(\mathrm{P}^A\mathrm{P}^C, A, C)$. Since $\delta_k^A = \Sigma\alpha_i^A\mu_i(\delta_k)^B$, $\alpha^A = \Sigma\alpha_i^A\mu_i(\delta_k)^B\pi_k(\alpha)^C$ and since $\mu_i(\delta_k)^B = \Sigma\beta_j^B\nu_j(\mu_i(\delta_k))^C$,

$$\alpha^A = \Sigma\alpha_i^A\beta_j^B\nu_j(\mu_i(\delta_k))^C\pi_k(\alpha)^C$$

Hence by (17) $\nu_j(\mu_i(\alpha)) = \Sigma\nu_j(\mu_i(\delta_k))\pi_k(\alpha)$, or

$$M_iN_j = \Sigma P_k\overline{\nu_j(\mu_i(\delta_k))}$$

is in the relations space of $(\mathrm{P}^A\mathrm{P}^C, A, C)$.

Now let $R_1, \cdots, R_s$ be a basis for the space over $\overline{\mathrm{P}}$ (on the right) generated by the product M_iN_j and write $\alpha R_k = \rho_k(\alpha)$. Then by expressing the elements M_iN_j in terms of the R_k we may replace the relations $\alpha^A = \Sigma\alpha_i^A\beta_j^B\nu_j(\mu_i(\alpha))^C$ by

$$\alpha^A = \sum_1^s \zeta_k\rho_k(\alpha)^C \tag{20}$$

where the $\zeta_k \in \Delta$. We wish to show that the $\zeta_k \in \mathrm{P}^A\mathrm{P}^C$. For this purpose we require the

LEMMA. *If $R_1, \cdots, R_s$ are endomorphisms in P that are linearly independent over $\bar{\mathrm{P}}$, then there exist elements λ_k, $k = 1, \cdots, s$ such that the matrix $(\lambda_k R_l)$ is non-singular.*

Suppose that we have already determined r elements λ_k such that the r vectors $(\lambda_k R_1, \cdots, \lambda_k R_s)$ are linearly independent. Then we assert that if $r < s$, there exists an element λ_{r+1} such that the $(r+1)$ vectors $(\lambda_k R_l)$ are linearly independent. For otherwise for each λ we have

$$\lambda R_l = \lambda_1 R_l \sigma_1(\lambda) + \cdots + \lambda_r R_l \sigma_r(\lambda), \qquad (l = 1, \cdots, s). \tag{21}$$

If $\Sigma \lambda_k R_l \sigma_k = 0$ for all l, by the linear independence of the vectors $(\lambda_k R_l)$ for $k = 1, \cdots, r$, each $\sigma_k = 0$. It follows that the σ in (21) are uniquely determined and so the correspondence $\lambda \rightarrow \sigma_k(\lambda) \equiv \lambda S_k$ is single valued. It is clear that S_k is an endomorphism of P and the relation (21) states that each R_l is a linear combination with coefficients in $\bar{\mathrm{P}}$ of the r endomorphisms S_k. This contradicts the linear independence of the R's and proves the lemma.

Now choose the λ's as in the lemma and write $\lambda_l{}^A = \Sigma \zeta_k \rho_k(\lambda_l)^C$. Since $(\rho_k(\lambda_l))$ is non-singular, there exist $\tau_{lk'}$ such that $\Sigma \rho_k(\lambda_l)^C \tau_{lk'}{}^C = \delta_{kk'}$. Then $\zeta_{k'} = \Sigma \lambda_l{}^A \tau_{lk'}{}^C$ is in $\mathrm{P}^A \mathrm{P}^C$. We now write $\zeta_k = \Sigma \delta_l{}^A \beta_{lk}{}^C$ and substitute in (20). This yields $\alpha^A = \Sigma \delta_l{}^A \beta_{lk}{}^C \rho_k(\alpha)^C$ and so by (19) $\pi_l(\alpha) = \Sigma \beta_{lk} \rho_k(\alpha)$. Thus $P_l = \Sigma R_k \beta_{lk}$ is in the space generated by the products $M_i N_j$. This completes the proof of

THEOREM 8. *The relations space of a product of two composites is the smallest space over $\bar{\mathrm{P}}$ containing all products. MN where M is in the relations space of the first composite and N is in the relations space of the second composite.*

This along with Theorem 4 proves that multiplication of composites is associative. Now it is readily seen that the relations space of the least common cover $(K, S, T) + (L, U, V)$ is the join of their respective spaces. It follows from Theorem 8 that the distributive laws hold: $[(K, S, T) + (L, U, V)] \times (M, X, Y) = (K, S, T) \times (M, X, Y) + (L, U, V) \times (M, X, Y)$ and $(M, X, Y) \times [(K, S, T) + (L, U, V)] = (M, X, Y) \times (K, S, T) + (M, X, Y) \times (L, U, V)$. We note also that any two composites (P^U, U, U) are identical and (P^U, U, U) satisfies the equation $(K, S, T) \times (\mathrm{P}^U, U, U) = (K, S, T) = (\mathrm{P}^U, U, U) \times (K, S, T)$. For this reason we shall call (P^U, U, U) the *identity* composite.

If we refer to the preceding section we see that the composite of a product of two representations or modules is the product of the corresponding composites.

9. Closed composites. We shall call a composite $\Gamma = (K, S, T)$ *closed* (under multiplication) if $(K, S, T) \geq (K, S, T) \times (K, S, T)$. By Theorem 3 and the considerations of the preceding section, (K, S, T) is closed if and only if its relations space $\mathfrak{A}(\Gamma)$ is a ring. A composite (K, S, T) will be called a *Galois composite* if 1) (K, S, T) is closed, 2) (K, S, T) is a cover of the identity composite (P^U, U, U) and 3) $(K, S, T) = (K, T, S)$. It will be a consequence of the results of **9** and **10** that any closed composite is a Galois composite. Hence the conditions 2) and 3) can be deleted in the definition of a Galois composite. We have preferred, however, to state them as separate conditions since they correspond to the existence of the identity and of inverses in a group.

We suppose now that $\Gamma = (K, S, T)$ is a closed composite and we let Φ_Γ denote the set of fixed elements relative to Γ. Let $\alpha_1, \cdots, \alpha_q$ be elements of P such that $\alpha_1^S, \cdots, \alpha_q^S$ form a basis for K over P^T. We assert that these elements form a basis for P over Φ_Γ. To prove this we consider the three-fold composite (Δ, A, B, C) that satisfies conditions 4. and 5. for (K, S, T) and $(L, U, V) = (K, S, T)$. In (K, S, T) we have $\alpha^S = \alpha_1^S \mu_1(\alpha)^T + \cdots + \alpha_q^S \mu_q(\alpha)^T$. Hence in Δ we have the relation $\alpha^A = \Sigma \alpha_i^A \mu_i(\alpha)^B$. Since (K, S, T) is closed, $(\mathrm{P}^A \mathrm{P}^C, A, C)$ is covered by (K, S, T). Hence $\alpha^A = \Sigma \alpha_i^A \mu_i(\alpha)^C$. Thus $\Sigma \alpha_i^A (\mu_i(\alpha)^B - \mu_i(\alpha)^C) = 0$. We have seen that the elements α_i^A are independent over $\mathrm{P}^B \mathrm{P}^C$. Hence this relation implies that $\mu_i(\alpha)^B = \mu_i(\alpha)^C$ and so each $\mu_i(\alpha) \in \Phi_\Gamma$. Thus each α in P is a linear combination with coefficients in Φ_Γ of the elements $\alpha_1, \cdots, \alpha_q$. Since the elements α_i^S are linearly independent over P^T, the elements α_i are linearly independent over Φ_Γ.

THEOREM 9. *Let $\Gamma = (K, S, T)$ be a closed composite, $(K : \mathrm{P}^T) = q$ and let Φ_Γ denote the field of fixed elements relative to Γ. Then $(\mathrm{P} : \Phi_\Gamma) = q$ and if $\alpha_1, \cdots, \alpha_q$ are q elements of P, they form a basis for P over Φ_Γ if and only if the elements $\alpha_1^S, \cdots, \alpha_q^S$ form a basis for K over P^T.*

The necessity of the condition is trivial. For if $\alpha_1, \cdots, \alpha_q$ from a basis for P over Φ_Γ, each $\alpha^S = \alpha_1^S \gamma_1^T + \cdots + \alpha_q^S \gamma_q^T$ where the $\gamma_i^T \in \Phi_\Gamma^T = \Phi_\Gamma^S$. Hence the α_i^S are linearly independent over P^T.

We consider now the relations ring $\mathfrak{A}(\Gamma)$. We have seen that its dimensionality over $\bar{\mathrm{P}}$ is q. Hence the dimensionality of $\mathfrak{A}(\Gamma)$ over $\bar{\Phi}_\Gamma$ is q^2. On the other hand we have seen that the transformations belonging to $\mathfrak{A}(\Gamma)$ commute with the elements of $\bar{\Phi}_\Gamma$, i. e., they are linear transformations in the space P over Φ_Γ. Since $(\mathrm{P} : \Phi_\Gamma) = q$, it follows that $\mathfrak{A}(\Gamma)$ is the complete set of linear transformations of P over Φ_Γ.

THEOREM 10. *If $\Gamma = (K, S, T)$ is a closed composite and Φ_Γ is its field of fixed elements, the relations space $\mathfrak{A}(\Gamma)$ is the complete ring of linear transformations of P over Φ_Γ.*

Suppose now that $\Gamma' = (K', S', T')$ is any composite of P which leaves the elements of Φ_Γ fixed. Then if N is any element of the relations space $\mathfrak{A}(\Gamma')$, N is a linear transformation in P over Φ_Γ. Hence by Theorem 10, $N \epsilon \mathfrak{A}(\Gamma)$, and so $\mathfrak{A}(\Gamma') \leq \mathfrak{A}(\Gamma)$. This implies the following

THEOREM 11. *Let Γ be a closed composite and Φ_Γ its field of fixed elements. Then if Γ' is any composite such that $\Phi_{\Gamma'} \geq \Phi_\Gamma$, $\Gamma' \leq \Gamma$.*

This, of course, implies that there is only one (in the sense of equivalence) closed composite having $\Phi = \Phi_\Gamma$ as its field of fixed elements.

It may be remarked that if $\Delta = (L, U, V)$ is any composite such that $(\mathrm{P} : \Phi_\Delta) = r < \infty$, then (L, U, V) is non-singular. For if we set $\Phi_\Delta = \Phi$, then $(\mathrm{P}^U : \Phi^U) = r = (\mathrm{P}^V : \Phi^V)$. Hence if $(L : \mathrm{P}^V) = q'$, $(L : \Phi^V) = rq'$ and since $\Phi^V = \Phi^U$, $(L : \Phi^U) = rq'$. It follows that $(L : \mathrm{P}^U) = q'$. A similar argument may be used to show that if $\mathfrak{S}$ is any double P-module with composite equivalent to Δ, then $\mathfrak{S}$ is non-singular. This may be stated as follows:

THEOREM 12. *If F is a self-representation of P such that the dimensionality of P over the field of fixed elements is finite, then F is similar to a non-singular self-representation.*

We again suppose that $\Delta = (L, U, V)$ is a composite such that $(\mathrm{P} : \Phi_\Delta) = r < \infty$. If Δ is not closed, we form the least common cover $\Delta^{(2)} = \Delta + \Delta \times \Delta$. Then the relations space $\mathfrak{A}(\Delta^{(2)}) > \mathfrak{A}(\Delta)$. It is readily seen that the field of fixed elements $\Phi_{\Delta^{(2)}} = \Phi_\Delta$ so that $(\mathrm{P} : \Phi_{\Delta^{(2)}}) = r$ also. If $\Delta^{(2)}$ is not closed we set $\Delta^{(3)} = \Delta + (\Delta \times \Delta) + (\Delta \times \Delta \times \Delta)$ and note that $\mathfrak{A}(\Delta^{(3)}) > \mathfrak{A}(\Delta^{(2)})$ and $\Phi_{\Delta^{(3)}} = \Phi_{\Delta^{(2)}}$. Since $\mathfrak{A}(\Delta)$, $\mathfrak{A}(\Delta^{(2)})$, $\mathfrak{A}(\Delta^{(3)})$ all have dimensionalities over $\bar{\Phi}_\Delta \leq r^2$, the dimensionality over $\bar{\Phi}_\Delta$ of the complete ring of linear transformations of P over Φ_Δ, this process leads after a finite number of steps to a closed composite $\Gamma = \Delta + (\Delta \times \Delta) + \cdots + (\Delta \times \cdots \times \Delta)$. By Theorem 10 we obtain

THEOREM 13. *Suppose that $\alpha \rightarrow (\alpha F_{kl})$ is a self-representation of P such that $(\mathrm{P} : \Phi) < \infty$ for Φ the field of fixed elements. Then if L is a linear transformation of P over Φ, L is expressible as a polynomial in the transformations F_{kl} with coefficients in $\bar{\mathrm{P}}$ the field of multiplications in P.*

10. The fundamental Galois correspondence. We suppose now that P is an arbitrary field and that Φ is a subfield of P such that $(P:\Phi) = q < \infty$. We take two copies P^S and P^T of P and form the direct product K of these fields relative to Φ.[7] Thus K is the set of sums $\Sigma\alpha^S\beta^T$, α^S in P^S and β^T in P^T where $\gamma^S = \gamma^T$ if $\gamma \epsilon \Phi$ and addition and multiplication are defined in the obvious way. The dimensionality $(K:\Phi^S) = q^2$ and $(K:P^S) = q = (K:P^T)$. We recall also that $P^S \wedge P^T = \Phi^S = \Phi^T$. It is evident that $\Gamma = (K, S, T)$, where S is the mapping $\alpha \to \alpha^S$ and T is the mapping $\alpha \to \alpha^T$, is a composite of P with itself. Since the mapping $\alpha^S \to \alpha^T$, $\alpha^T \to \alpha^S$ is an automorphism in K, (K, S, T) is symmetric. Since $P^S \wedge P^T = \Phi^S = \Phi^T$, the field Φ_Γ of fixed elements is Φ. Now let (L, U, V) be any composite of P leaving the elements of Φ fixed. Suppose that $\Sigma\alpha^S\beta^T = 0$ in K. Then if $\alpha_1, \cdots, \alpha_q$ form a basis for P over Φ, the elements $\alpha_i{}^S\alpha_j{}^T$ form a basis for K over $\Phi^S = \Phi^T$ and the elements $\alpha_i{}^U\alpha_j{}^V$ are generators of L over $\Phi^U = \Phi^V$. We replace α^S by $\Sigma\gamma_i{}^S\alpha_i{}^S$, γ_i in Φ and β^T by $\Sigma\delta_j{}^T\alpha_j{}^T$, δ_j in Φ and substitute in the relation $\Sigma\alpha^S\beta^T = 0$. Then the coefficients of the products $\alpha_i{}^S\alpha_j{}^T$ in the resulting expression are all 0. Hence if we substitute $\alpha^U = \Sigma\gamma_i{}^U\alpha_i{}^U$ and $\beta^V = \Sigma\delta_j{}^V\alpha_j{}^V$ in $\alpha^U\beta^V$, we see that $\Sigma\alpha^U\beta^V = 0$. We have therefore proved that (K, S, T) is a cover for (L, U, V). This shows, in particular, that $(K, S, T) \geq (K, S, T) \times (K, S, T)$ and $(K, S, T) \geq (P^U, U, U)$.

THEOREM 14. *If* P *is a field and* Φ *a subfield such that* $(P:\Phi) = q < \infty$, *then the direct product of* P *over* Φ *with itself determines a Galois composite whose field of fixed elements is* Φ.

Now suppose that Γ is any closed composite and let Φ_Γ be the subfield of P of fixed elements under Γ. We have seen that $(P:\Phi_\Gamma) < \infty$ and hence we may form the direct product Γ' of P over Φ_Γ by itself. By Theorem 11, $\Gamma' \leq \Gamma$ and by what we have just proved $\Gamma \leq \Gamma'$. Hence Γ is equivalent to Γ' and so we have proved

THEOREM 15. *Any closed composite is a Galois composite.*

As a consequence of Theorems 9, 11, and 14 we have the following fundamental

THEOREM 16. *Let* P *be a fixed field and* Γ *a Galois composite of* P. *If* Φ_Γ *denotes the field of fixed elements under* Γ, *then* P *is finite over* Φ_Γ *and the correspondence* $\Gamma \to \Phi_\Gamma$ *is* $(1-1)$ *between the Galois composites and the subfields* Φ *over which* P *is finite.* $\Gamma_1 \geqq \Gamma_2$ *if and only if* $\Phi_{\Gamma_1} \leqq \Phi_{\Gamma_2}$.

---

[7] For the definition and properties of the direct product see, for example, *R*, p. 88.

11. Decomposition of composites. Let $\Gamma = (K, S, T)$ be an arbitrary composite. Since K is a commutative algebra with a finite basis over P^T, we may decompose K as a direct sum

$$K = K_1 \oplus \cdots \oplus K_s \tag{21}$$

of indecomposable algebras K_i. The K_i are uniquely determined. Moreover if B is any ideal in K, $B = B_1 \oplus \cdots \oplus B_s$ where $B_i = B \wedge K_i$. Hence if N is the radical of K, $N = N_1 \oplus \cdots \oplus N_s$ where $N_i = N \wedge K_i$ is the radical of K_i. We recall now that any indecomposable commutative algebra is completely primary in the sense that the difference algebra with respect to its radical is a field.[8] Any ideal of such an algebra is contained in the radical. It follows that the homomorphic image of such an algebra is also completely primary and hence is also indecomposable. These results apply in particular to the algebras K_i.

Corresponding to the decomposition (21) we write

$$1 = e_1 + \cdots + e_s$$

where

$$e_i^2 = e_i, \quad e_i e_j = 0 \text{ if } i \neq j.$$

Then $K_i = Ke_i$. The mapping $k \to ke_i$ is a homomorphism E_i of K into K_i. We set $S_i = SE_i$, $T_i = TE_i$. These are isomorphisms between P and subfields P^{S_i} and P^{T_i} of K_i. Since $K = \mathrm{P}^S\mathrm{P}^T$, $K_i = \mathrm{P}^{S_i}\mathrm{P}^{T_i}$. Evidently $(K : \mathrm{P}^T) = \Sigma(K_i : \mathrm{P}^T)$ and since $k_i\alpha^T = k_i\alpha^{T_i}$ if $k_i \in K_i$, $(K_i : \mathrm{P}^T) = (K_i : \mathrm{P}^{T_i})$. Hence $(K_i : \mathrm{P}^{T_i})$ is finite. Thus (K_i, S_i, T_i) is a composite of P. It is evident that (K, S, T) is the least common cover of these composites. We shall now show that the composites (K_i, S_i, T_i) are *disjoint* in the sense that there exists no composite (L, U, V) which is covered by both (K_i, S_i, T_i) and the least common cover of all the (K_j, S_j, T_j) for $j \neq i$. For let (L, U, V) be such a composite. Suppose that $e_i = \Sigma\alpha^S\beta^T$. Then $e_i = e_i^2 = \Sigma\alpha^{S_i}\beta^{T_i}$ and $0 = e_ie_j = \Sigma\alpha^{S_j}\beta^{T_j}$ for all $j \neq i$. In L we have $1^U = \Sigma\alpha^U\beta^V$ and $0 = \Sigma\alpha^U\beta^V$ and this contradiction proves our assertion.

If B is an ideal in K and $k \to \bar{k}$ denotes the natural homomorphism between K and $\bar{K} = K - B$, it is clear that $(\bar{K}, \bar{S}, \bar{T})$ where $\alpha^{\bar{S}} = \overline{\alpha^S}$, $\beta^{\bar{T}} = \overline{\beta^T}$ is a composite of P covered by (K, S, T) and, as we have remarked, any composite covered by (K, S, T) can be obtained in this way. If C is an ideal containing B, it is readily seen that the composite $(K - B, \bar{S}, \bar{T})$ is a cover of $(K - C, \bar{S}, \bar{T})$. Now since any ideal B_i of K_i is contained in the radical

[8] Cf. Theorem 3, Chapter 4 of *R*.

N_i, this shows that any composite covered by (K_i, S_i, T_i) is a cover of the composite $(K_i - N_i, \bar{S}_i, \bar{T}_i)$. Thus it is impossible to find disjoint composites which are covered by (K_i, S_i, T_i).

From the decomposition $K = K_1 \oplus \cdots \oplus K_s$ we obtain $K - B = \bar{K} = \bar{K}_1 + \cdots + \bar{K}_s$. Also $B = B_1 \oplus \cdots \oplus B_s$ where $B_i = B \wedge K_i$. Hence if $\bar{k}_1 + \bar{k}_2 + \cdots + \bar{k}_s = 0$, $k_1 + k_2 + \cdots + k_s = b_1 + b_2 + \cdots + b_s$ where the $b_i \epsilon B_i$. Then $k_i = b_i$ is in B_i and $\bar{k}_i = 0$. Thus $\bar{K} = \bar{K}_1 \oplus \cdots \oplus \bar{K}_s$. Each $\bar{K}_i$ is indecomposable since it is the homomorphic image of the indecomposable algebra K_i. We suppose that $\bar{K}_i \neq 0$ if $i \leq r$ and that $\bar{K}_i = 0$ if $i > r$. We now denote the mapping $k \to \bar{k}$ by H, the mapping $\bar{k} \to \bar{k}_i$ by $\bar{E}_i$ and we set $\bar{S}_i = SH\bar{E}_i$, $\bar{T}_i = TH\bar{E}_i$. Then $(\bar{K}_i, \bar{S}_i, \bar{T}_i)$ is a composite of P with itself. Moreover, these composites are obtained from $(\bar{K}, \bar{S}, \bar{T})$ in the same way that the (K_i, S_i, T_i) are obtained from (K, S, T). We assert now that $(\bar{K}_i, \bar{S}_i, \bar{T}_i)$ is covered by (K_i, S_i, T_i). For suppose that $\Sigma \alpha^{S_i} \beta^{T_i} = 0$. Then if $k = \Sigma \alpha^S \beta^T$, $k_i = 0$. Now in the decomposition $\bar{k} = \bar{k}_1 + \cdots + \bar{k}_s$, $\bar{k}_i$ is the coset of k_i. Hence $\bar{k}_i = 0$. Thus $\Sigma \alpha^{\bar{S}_i} \beta^{\bar{T}_i} = (\Sigma \alpha^S \beta^T)^{HE_i} = \bar{k}_i = 0$ and this proves our assertion. In particular we see that if $(\bar{K}, \bar{S}, \bar{T})$ is indecomposable, i. e. if $r = 1$, then $(\bar{K}, \bar{S}, \bar{T})$ is covered by one of the composites (K_i, S_i, T_i).

Now suppose that (K, S, T) is the least common cover of the composites (K'_j, S'_j, T'_j), $j = 1, \cdots, s'$ which are disjoint and *indecomposable* in the sense that they are not least common covers of disjoint composites. Then each algebra K'_j is indecomposable and since (K, S, T) is a cover of (K'_j, S'_j, T'_j) one of the (K_i, S_i, T_i) is a cover of (K'_j, S'_j, T'_j). Since the (K_i, S_i, T_i) are disjoint, only one of these, say $(K_{\bar{j}}, S_{\bar{j}}, T_{\bar{j}})$, is a cover for (K'_j, S'_j, T'_j). Since no two composites covered by (K_j, S_j, T_j) are disjoint, it follows that if $j \neq k$, then $\bar{j} \neq \bar{k}$. If we re-arrange the (K_j, S_j, T_j), we may suppose that $\bar{j} = j$. We wish to show that (K_j, S_j, T_j) and (K'_j, S'_j, T'_j) are equivalent and so we assume that this is not the case. Then there is a relation $\Sigma \lambda^{S'_j} \mu^{T'_j} = 0$ such that $\Sigma \lambda^{S_j} \mu^{T_j} \neq 0$. If $e_j = \Sigma \alpha^S \beta^T$, $e_j = \Sigma \alpha^{S_j} \beta^{T_j}$ and $\Sigma \lambda^{S_j} \alpha^{S_j} \mu^{T_j} \beta^{T_j} \neq 0$. Since $e_j e_k = 0$ if $j \neq k$, $\Sigma \alpha^{S_k} \beta^{S_k} = 0$ and hence $\Sigma \lambda^{S_k} \alpha^{S_k} \mu^{T_k} \beta^{T_k} = 0$. Thus we may suppose at the start that $\Sigma \lambda^{S_k} \mu^{T_k} = 0$ for $k \neq j$. It follows that $\Sigma \lambda^{S'_k} \mu^{T'_k} = 0$ and hence that $\Sigma \lambda^S \mu^T = 0$ and this contradicts the fact that $\Sigma \lambda^{S_j} \mu^{T_j} \neq 0$. Now it is clear that $s' = s$. For otherwise there exists a (K_i, S_i, T_i) which is covered by the least common cover of the (K_j, S_j, T_j) for $j \neq i$. We have therefore proved the following:

THEOREM 17. *Any composite (K, S, T) is expressible in one and only one way as the least common cover of disjoint indecomposable composites.*

We shall call the *indecomposable* composites (K_i, S_i, T_i) the *indecomposable components* of (K, S, T). The argument given above proves

THEOREM 18. *If* (L, U, V) *is covered by* (K, S, T) *then each indecomposable component of* (L, U, V) *is covered by an indecomposable component of* (K, S, T).

Suppose now that (K, S, T) is a Galois composite. Then we have seen that any composite covered by (K, S, T) is non-singular. This applies in particular to the indecomposable components (K_i, S_i, T_i). Consider now the inverses (K_i, T_i, S_i). It is clear that these are indecomposable and disjoint and that their least common cover is (K, T, S). Since $(K, S, T) = (K, T, S)$ it follows that the set of inverses (K_i, T_i, S_i) coincides with the set (K_i, S_i, T_i). We observe next that since $(K, S, T) \times (K, S, T) \leq (K, S, T)$ and since $(K, S, T) \times (K, S, T)$ is a cover of every product $(K_i, S_i, T_i) \times (K_j, S_j, T_j)$, the indecomposable components of these products are covered by suitable ones of the (K_k, S_k, T_k). We note finally that since (K, S, T) is a cover of (P^U, U, U) one of the (K_i, S_i, T_i) is a cover of this composite. Conversely suppose that (K, S, T) is any composite whose indecomposable components (K_i, S_i, T_i) satisfy

1. Each (K_i, S_i, T_i) is non-singular,
2. One of the (K_i, S_i, T_i), say (K_1, S_1, T_1), is a cover of the identity composite (P^U, U, U),
3. For each (K_i, S_i, T_i) the inverse (K_i, T_i, S_i) is an indecomposable component,
4. The indecomposable components of $(K_i,\ S_i,\ T_i) \times (K_j,\ S_j,\ T_j)$ are covered by the (K_k, S_k, T_k).

Then since $(K, S, T) \times (K, S, T)$ is the least common cover of the products $(K_i, S_i, T_i) \times (K_j, S_j, T_j)$, (K, S, T) is a cover of $(K, S, T) \times (K, S, T)$. It is evident also that $(K, S, T) \geq (P^U, U, U)$ and that (K, S, T) is symmetric.

THEOREM 19. *Conditions* 1.-4. *on the indecomposable components of a composite are necessary and sufficient that the composite be a Galois composite.*

12. Separable fields. We shall call a composite (K, S, T) *simple* if K is a field. In this case the only composite covered by (K, S, T) is (K, S, T) itself. (K, S, T) is *semi-simple* if its indecomposable components are simple. If the components of (K, S, T) are (K_i, S_i, T_i), $i = 1, \cdots, s$, it follows that

any composite covered by (K, S, T) is the least common cover of certain of the (K_i, S_i, T_i).

We shall prove first the following

THEOREM 20. *Let* P *be a field,* Φ *a subfield such that* $(\mathrm{P}:\Phi) = q < \infty$ *and let* $\Gamma = (K, S, T)$ *be the Galois composite whose field of fixed elements* $\Phi_\Gamma = \Phi$. *Then a necessary and sufficient condition that* P *be separable over* Φ *is that* Γ *be semi-simple.*

Sufficiency. Let α be any element of P and set $\Sigma = \Phi(\alpha^p)$ where p is the characteristic of Φ. Consider the Galois composite $\Delta = (L, U, V)$ of P having $\Sigma = \Phi_\Delta$ as its field of fixed elements. Since Δ is covered by Γ, it is semi-simple. Now $(\alpha^U)^p = (\alpha^p)^U = (\alpha^p)^V = (\alpha^V)^p$. Hence $(\alpha^U - \alpha^V)^p = 0$ and so $\alpha^U = \alpha^V$. Thus $\alpha \in \Sigma = \Phi(\alpha^p)$ and hence α is separable.

Necessity. Suppose that P is separable over Φ. Then there exists a primitive element α in P such that $\mathrm{P} = \Phi(\alpha)$. Let (L, U, V) be an indecomposable composite and let $\phi^V(\lambda)$ be the minimum polynomial of α^U over the field P^V. Since L is an indecomposable algebra $\phi^V(\lambda) = \psi^V(\lambda)^e$ where $\psi^V(\lambda)$ is irreducible. For if $\phi^V(\lambda) = \psi_1{}^V(\lambda)\psi_2{}^V(\lambda)$ where $(\psi_1{}^V(\lambda), \psi_2{}^V(\lambda)) = 1$, $\psi_1{}^V(\alpha^U)$ is a zero-divisor $\neq 0$ in L and since any zero-divisor of a completely primary algebra is contained in the radical $\psi_1{}^V(\alpha^U)^f = 0$. This implies that $\psi_1{}^V(\lambda)^f$ is divisible by $\psi_1{}^V(\lambda)\psi_2{}^V(\lambda)$ contrary to $(\psi_1{}^V(\lambda), \psi_2{}^V(\lambda)) = 1$. Now let $\mu(\lambda)$ be the minimum polynomial of α over Φ. Then $\mu^V(\lambda) = \phi^V(\lambda)\phi_1{}^V(\lambda) = \psi^V(\lambda)^e\psi_1{}^V(\lambda)$. It follows from this that $(\mu(\lambda), \mu'(\lambda)) \neq 1$ if $e > 1$. Thus $e = 1$ and α^U satisfies an irreducible polynomial over P^V. Hence $L = \mathrm{P}^V(\alpha^U)$ is a field. We have therefore proved that any indecomposable composite of P is irreducible and hence any composite is semi-simple.

We now recall the definition of a *hypergroup* (with an identity) H as a system in which a product of pairs equal to a subset of H is defined. If A and B are subsets of H, we define AB to be the set of elements contained in all products ab, a in A and b in B. It is assumed that 1) the product is associative: the set $(ab)c = a(bc)$, 2) there exists an identity 1 in H such that $a1 = 1a = a$ for all a in H and 3) for each a there is an inverse b such that ab and ba contain 1.

Suppose now that H is a set of non-singular simple composites of P having the following properties: 1) If Γ_1 and Γ_2 belong to H, then $\Gamma_1 \times \Gamma_2$ is the least common cover of certain Γ_i in H. 2) H contains the identity composite. 3) H contains the inverse Γ^{-1} of any Γ in H. Then if we define $\Gamma_1\Gamma_2$ to be the set of simple composites contained in H and covered by $\Gamma_1 \times \Gamma_2$, it is easy to see that H is a hypergroup. We shall therefore call a set of non-singular

simple composites with the properties 1), 2) and 3) a *hypergroup of simple composites.*

Now let H be a finite hypergroup of simple composites and let $\Gamma = (K, S, T)$ be the least common cover of all the Γ_i in H. If (K_i, S_i, T_i) are the indecomposable components of Γ, it is evident that each Γ_i is covered by one of the (K_i, S_i, T_i) no two Γ_i are covered by the same (K_i, S_i, T_i) and no two (K_i, S_i, T_i) cover the same Γ_i. It follows that the Γ_i coincide with the (K_i, S_i, T_i). Hence by Theorem 19, (K, S, T) is a Galois composite and since its indecomposable components are simple, (K, S, T) is semi-simple. Let Φ_H be the field of fixed elements relative to the Γ_i. Then $\Phi_H = \Phi_\Gamma$ and hence P is finite and separable over Φ_H. Conversely suppose that P is finite and separable over Φ and let Γ be the Galois composite such that $\Phi_\Gamma = \Phi$. Then we have seen that Γ is semi-simple and it follows from Theorem 19 that the indecomposable components Γ_i of Γ form a finite hypergroup H of simple composites. Evidently $\Phi_H = \Phi$. We have therefore proved

THEOREM 21. *Let* P *be a fixed field and* H *a finite hypergroup of simple composites of* P. *Then if* Φ_H *denotes the field of fixed elements under all the composites in* H, P *is finite and separable over* Φ_H. *The correspondence* $H \rightarrow \Phi_H$ *is* $(1-1)$ *between the finite hypergroups of simple composites of* P *and the subfields* Φ_H *over which* P *is finite and separable.* $H_1 \geq H_2$ *if and only if* $\Phi_{H_1} \leq \Phi_{H_2}$.[9]

13. Normal fields. We shall call a composite (L, U, V) *one-dimensional* if $(L : \mathrm{P}^V) = 1$. Evidently this implies that (L, U, V) is simple. With this definition we have

THEOREM 22. *A necessary and sufficient condition that a field* P *finite over a subfield* Φ *be normal over* Φ *is that every simple composite* (L, U, V), *whose field of fixed elements contains* Φ, *is one-dimensional.*

Suppose that P is normal over Φ and that (L, U, V) is a simple composite whose field of fixed elements contains Φ. Let α be an element of P and let $\mu(\lambda)$ be its minimum polynomial over Φ. Since P is normal, $\mu(\lambda) = (\lambda - \alpha_1) \cdots (\lambda - \alpha_m)$, $\alpha_1 = \alpha$, in $\mathrm{P}[\lambda]$. Hence $\mu^V(\lambda) = \Pi(\lambda - \alpha_i^V)$. Since $\mu^V(\alpha^U) = 0$, $\Pi(\alpha^U - \alpha_i^V) = 0$ and since L is a field $\alpha^U = \alpha_i^V$ for a suitable i. Thus $\mathrm{P}^U \leq \mathrm{P}^V$ and $(L : \mathrm{P}^V) = 1$.

Next suppose that for every simple (L, U, V) whose field of fixed elements contains Φ, $(L : \mathrm{P}^V) = 1$. Consider the Galois composite $\Gamma = (K, S, T)$ such

---

[9] Cf. Kaloujnine, *loc. cit.*[3].

that $\Phi_\Gamma = \Phi$. Let $K = K_1 \oplus \cdots \oplus K_s$ where the K_i are indecomposable. If N is the radical of K, $N = N_1 \oplus \cdots \oplus N_s$, N_i the radical of K_i. We define the S_i, T_i as in **11** and consider the simple composite $(K_i - N_i, \bar{S}_i, \bar{T}_i)$ where $\bar{S}_i$, $\bar{T}_i$ are obtained by first applying S_i, T_i and then the natural homomorphism between K_i and $K_i - N_i$. By our assumption for any α in P, $\alpha^{\bar{S}_i} = \beta_i^{\bar{T}_i}$ for a suitable β_i. Hence $(\alpha^{S_i} - \beta_i^{T_i})^{n_i} = 0$ for some n_i. We assume that n_i is minimal and we may assume also that the notation has been chosen so that $\beta_1 = \cdots = \beta_{r_1} \equiv \delta_1 \neq \beta_{r_1+1} = \cdots = \beta_{r_1+r_2} = \delta_2 \neq \cdots$ and that $m_1 = n_1 \geq n_2 \geq \cdots \geq n_{r_1}$; $m_2 = n_{r_1+1} \geq n_{r_1+2} \geq \cdots \geq n_{r_1+r_2}; \cdots$. Consider the polynomial $\mu^T(\lambda) = (\lambda - \delta_1^T)^{m_1} \cdots (\lambda - \delta_t^T)^{m_t}$. We wish to prove that $\mu^T(\lambda)$ is the minimum polynomial over P^T satisfied by α^S. We note first that $(\alpha^{S_i} - \delta_1^{T_i})^{m_1} \cdots (\alpha^{S_i} - \delta_t^{T_i})^{m_t}$ contains the factor $(\alpha^{S_i} - \beta_i^{T_i})^{n_i} = 0$. Since (K, S, T) is the least common cover of the (K_i, S_i, T_i) this implies that $\mu^T(\alpha^S) = 0$. Now let $\nu^T(\lambda)$ be the minimum polynomial of α^S over P^T. We recall that if $1, \alpha, \cdots, \alpha^{r-1}$ are linearly independent over Φ, then $1, \alpha^S, \cdots, (\alpha^S)^{r-1}$ are linearly independent over P^T. This implies that $\nu^T(\lambda)$ has coefficients in $\Phi^T = \Phi^S$. Hence $\nu(\lambda)$ is the minimum polynomial of α over Φ. Since $\nu^T(\alpha^S) = 0$, $\nu^{T_i}(\alpha^{S_i}) = 0$. This implies that $\nu^{T_i}(\lambda)$ is divisible by $(\lambda - \beta_i^{T_i})^{n_i}$ and hence that $\nu^T(\lambda)$ is divisible by $(\lambda - \beta_i^T)^{n_i}$. It follows that $\nu^T(\lambda)$ is divisible by $\mu^T(\lambda)$ and since $\nu^T(\lambda)$ is minimal, $\mu^T(\lambda) = \nu^T(\lambda)$. From the factorization $\mu^T(\lambda) = \Pi(\lambda - \delta_j^T)^{m_j}$ we obtain $\mu(\lambda) = \Pi(\lambda - \delta_j)^{m_j}$. Thus the minimum polynomial of α over Φ factors into linear factors in $P[\lambda]$ and so P is normal over Φ.

Let (L, U, V) be any non-singular one dimensional composite of P. Then $L = P^V$. Since $(L : P^U) = 1$ also, $L = P^U$. If we apply the isomorphism V^{-1} to L, we see that (L, U, V) is equivalent to the composite $(P, A, 1)$ where $A = UV^{-1}$ is an automorphism in P and 1 is the identity automorphism. Conversely if A is any automorphism, $(P, A, 1)$ is a non-singular composite. It is clear that $(P, A, 1) = (P, 1, A^{-1})$. Hence the inverse of $(P, A, 1)$ is $(P, A^{-1}, 1) = (P, 1, A)$. It follows directly from the definition of the product that $(P, A, 1) \times (P, B, 1) = (P, A, 1) \times (P, 1, B^{-1}) = (P, A, B^{-1}) = (P, AB, 1)$. Thus the totality of non-singular one-dimensional composites of P is a group under multiplication isomorphic to the group of automorphisms of P.

Suppose now that H is a finite hypergroup of one dimensional composites. Then it is clear that H is a group and by Theorems 21 and 22, P is finite, separable and normal over Φ_H. Conversely if P is finite, separable and normal over Φ, then the indecomposable components of the Galois composite Γ such that $\Phi_\Gamma = \Phi$ form a group H under multiplication. If $(P, A, 1)$ is one of

the simple components of Γ then A is an automorphism of P that leaves the elements of Φ fixed. On the other hand if A is such an automorphism of P, $(\mathrm{P}, A, 1)$ is a composite leaving the elements of Φ fixed. Hence $(\mathrm{P}, A, 1)$ is covered by Γ and therefore $(\mathrm{P}, A, 1)$ is one of the indecomposable components of Γ. This completes the proof of the classical correspondence:

THEOREM 23. *If* P *is an arbitrary field, there is a* $(1-1)$ *correspondence between the finite groups H of automorphisms in* P *and the subfields Φ_H over which* P *is finite, separable and normal, namely, Φ_H is the set of fixed elements under the automorphisms of H and H is the complete set of automorphisms leaving the elements of Φ fixed.*

We recall that $(K:\mathrm{P}^T) = \Sigma(K_i:\mathrm{P}^{T_i})$. If P is separable and normal over Φ_Γ, each $(K_i;\mathrm{P}^{T_i}) = 1$ and hence $(\mathrm{P}:\Phi_\Gamma) = (K:\mathrm{P}^T)$ is the number of components (K_i, S_i, T_i). It follows that $(\mathrm{P}:\Phi_\Gamma)$ is the order of the Galois group of P over Φ_Γ.

14. Simple extensions. Suppose that $\mathrm{P} = \Phi(\alpha)$ a simple extension of Φ and let $\mu(\lambda)$ be the minimum polynomial of α over Φ. Let $\Gamma = (K, S, T)$ be the Galois composite whose field of fixed elements $\Phi_\Gamma = \Phi$. Then the minimum polynomial of α^S over P^T is $\mu^T(\lambda)$ and the degree of $\mu^T(\lambda)$ is the dimensionality q of K over P^T. If $\Delta = (L, U, V)$ is any composite such that $\Phi_\Delta \geqq \Phi$, Γ is a cover of Δ and hence L is generated by α^U over P^V. Thus if $\nu^V(\lambda)$ is the minimum polynomial of α^U over P^V and r is the degree of $\nu^V(\lambda)$ then the elements $1, \alpha^U, \cdots, (\alpha^U)^{r-1}$ form a basis for L over P^V. Since $\mu^V(\alpha^U) = 0$, $\nu^V(\lambda)$ is a factor of $\mu^V(\lambda)$ and hence the polynomial $\nu(\lambda)$ in $\mathrm{P}[\lambda]$ is a factor of $\mu(\lambda)$. Thus we have associated with the composite Δ the factor $\nu(\lambda)$ of $\mu(\lambda)$ in $\mathrm{P}[\lambda]$. The composite $\Delta_1 \geqq \Delta_2$ if and only if the associated factor $\nu_1(\lambda)$ is divisible by $\nu_2(\lambda)$. We shall show next that every factor $\nu(\lambda)$ of $\mu(\lambda)$ in $\mathrm{P}[\lambda]$ arises in this way from some composite. For if $\mu(\lambda) = \nu(\lambda)\nu_1(\lambda)$ and B is the ideal in K generated by $\nu^T(\alpha^S)$ then $(K - B, \bar{S}, \bar{T})$ is the required composite. The correspondence between composites Δ such that $\Phi_\Delta \geqq \Phi$ and the factors $\nu(\lambda)$ of $\mu(\lambda)$ in $\mathrm{P}[\lambda]$ is therefore $(1-1)$. It is readily seen that the indecomposable components of Γ correspond to the prime power factors $\pi_i(\lambda)^{e_i}$ of $\mu(\lambda) = \pi_1(\lambda)^{e_1} \cdots \pi_s(\lambda)^{e_s}$ in $\mathrm{P}[\lambda]$.

Let $\nu(\lambda) = \lambda^m - \beta_1\lambda^{m-1} - \cdots - \beta_m$ be a factor of $\mu(\lambda)$ and let (L, U, V) be the corresponding composite. Then if we turn L into a double P-module by defining $\alpha x = \alpha^U x = x\alpha^U$ and $x\alpha = \alpha^V x = x\alpha^V$, it may be verified that the matrix of α^U relative to the basis $1, \alpha^U, \cdots, (\alpha^U)^{m-1}$ is

$$\alpha^F \doteq \begin{pmatrix} 0 & \cdot & \cdot & \cdot & \cdot & \beta_m \\ 1 & & & & & \cdot \\ & \cdot & & & & \cdot \\ & & \cdot & & & \cdot \\ & & & \cdot & & \cdot \\ & & & & 1 & \beta_1 \end{pmatrix}. \tag{22}$$

If $\pi(\lambda) = \lambda^n - \delta_1\lambda^{n-1} - \cdot \cdot \cdot - \delta_n$ is a second factor of $\mu(\lambda)$, it determines in the same way a composite and a self-representation in which α is represented by the matrix

$$\alpha^G = \begin{pmatrix} 0 & \cdot & \cdot & \cdot & \cdot & \delta_n \\ 1 & & & & & \cdot \\ & \cdot & & & & \cdot \\ & & \cdot & & & \cdot \\ & & & \cdot & & \cdot \\ & & & & 1 & \delta_1 \end{pmatrix}.$$

The elements β_i are polynomials in α with coefficients in Φ. If we replace the β_i in α^F by the corresponding polynomials in α^G, we obtain the matrix $\alpha^{F\times G}$ representing α in the product representation. If $\rho(\lambda)$ is the minimum polynomial of $\alpha^{F\times G}$, $\rho(\lambda)$ is a factor of $\mu(\lambda)$ and the composite associated with $\rho(\lambda)$ is the product of the composites associated with $\nu(\lambda)$ and the composite associated with $\pi(\lambda)$.

If we apply the theory of a single linear transformation we see that any self-representation $\alpha \rightarrow \alpha^E$ is decomposable into "cyclic" self-representations E_i where α^{E_i} has the form (22).

THE JOHNS HOPKINS UNIVERSITY.

ALGEBRAS DERIVED BY NON-ASSOCIATIVE MATRIX MULTIPLICATION.*

By A. A. Albert.

1. Introduction. There are four ways to form an n-rowed matrix whose determinant is the product of the determinants of two n-rowed matrices, and only one of these, the row by column product, is an associative product. The row by row, column by column, and column by row products determine algebras which are not associative and it has recently been suggested to the author, in conversation, that these algebras have applications to some problems of physics.

We shall study the structure of such algebras here with particular attention to those algebras obtained by the three non-associative products from associative algebras $\mathfrak{C}$ such that $\mathfrak{C}$ contains the transpose x' of every x of $\mathfrak{C}$. We shall indeed obtain a general structure theory not merely for such algebras but for the case where $\mathfrak{C}$ is any algebra with an involution J. Thus our results will include the case where J is the conjugate transpose operation. We shall also show that there are linear spaces of real matrices closed under row by row (or column by column) multiplication and not under row by column multiplication, but that these row by row algebras cannot be semi-simple.

2. Row and column algebras. An algebra $\mathfrak{C}$ over a field $\mathfrak{F}$ is a linear space of finite order over $\mathfrak{F}$ which is closed with respect to an operation of multiplication which is a linear transformation $a \rightarrow ax$ over $\mathfrak{F}$ on $\mathfrak{C}$. We may define other algebras whose quantities are those of $\mathfrak{C}$ but in which multiplication is defined by different linear transformations. In particular let A, B, C be any non-singular transformations on $\mathfrak{C}$ and define an algebra $\mathfrak{C}_0$ whose products $a \cdot x$ are given in terms of products in $\mathfrak{C}$ by

$$a \cdot x = \{(aA)(xB)\}C. \tag{1}$$

Then $\mathfrak{C}$ and $\mathfrak{C}_0$ are said to be *isotopic*.[1] We shall consider the subalgebras of certain isotopes of involutorial algebras.

---

* Received January 29, 1943.

[1] For an equivalent definition in a slightly different form see my "Non-associative algebras I. Fundamental concepts and isotopy," *Annals of Mathematics*, vol. 43 (1942), pp. 685-707.

An involution [2] J over $\mathfrak{F}$ of an algebra $\mathfrak{C}$ over a field $\mathfrak{F}$ is a linear transformation J over $\mathfrak{F}$ on $\mathfrak{C}$ such that J^2 is the identity transformation,

$$(ax)J = (xJ)(aJ) \tag{2}$$

for every a and x in C. Since J is non-singular the algebras

$$\mathfrak{C}_\rho = \mathfrak{C}_\rho(J), \quad \mathfrak{C}_\kappa = \mathfrak{C}_\kappa(J), \quad \mathfrak{C}_{\kappa\rho} = \mathfrak{C}_{\kappa\rho}(J), \tag{3}$$

defined, respectively, by the product operations given in

$$x \cdot y = x(yJ), \quad (x, y) = (xJ)y, \quad [x, y] = (xJ)(yJ), \tag{4}$$

are isotopic to $\mathfrak{C}$.

In the special case where $\mathfrak{C}$ is the algebra of all t-rowed square matrices and J is the operation of transposition the product $x \cdot y$ is the row by row matrix product. This suggests the term *row* algebra (relative to $\mathfrak{C}$ and J) for any subalgebra of $\mathfrak{C}_\rho(J)$. Similarly we shall call the subalgebras of $\mathfrak{C}_\kappa(J)$ *column* algebras and the subalgebras of $\mathfrak{C}_{\kappa\rho}(J)$ *column by row* algebras.

A row algebra is thus a linear subspace $\mathfrak{A}$ of order n over $\mathfrak{F}$ of an algebra $\mathfrak{C}$ such that

$$x \cdot y = x(yJ) \tag{5}$$

is in $\mathfrak{A}$ for every x and y of $\mathfrak{A}$. In general yJ is not in $\mathfrak{A}$ and $\mathfrak{A}$ need not form a subalgebra of $\mathfrak{C}$. We shall give an example of such an algebra later. Thus (5) does not necessarily define $\mathfrak{A}$ as an isotope of a subalgebra of $\mathfrak{C}$. However J is non-singular and the mapping $x \to xJ$ of $\mathfrak{A}$ on another subspace $\mathfrak{A}J$ of $\mathfrak{C}$ is one to one. If x and y are in $\mathfrak{A}$ we have

$$(x \cdot y)J = \{x(yJ)\}J = \{(yJ)J\}(xJ) = (yJ, xJ).$$

It follows that $\mathfrak{A}J$ is a column algebra and that the correspondence $x \to xJ$ is an anti-isomorphism. We have proved

THEOREM 1. *Every column algebra is anti-isomorphic to a row algebra. In particular, every $\mathfrak{C}_\rho(J)$ is anti-isomorphic to $\mathfrak{C}_\kappa(J)$.*

This result reduces our study to that of row algebras and of column by row algebras. We shall therefore omit entirely all mention of column algebras henceforth *in our proofs*.

---

[2] Cf. my "Involutorial simple algebras and real Riemann matrices," *Annals of Mathematics*, vol. 36 (1935), pp. 886-964.

It should also be noted that $(x \cdot y)J = y(xJ) = y \cdot x$ and thus the self correspondence $x \rightarrow xJ$ does not in general carry $x \cdot y$ into either $xJ \cdot yJ$ or $yJ \cdot xJ$. Hence J is, in general, neither an automorphism or anti-automorphism[3] of $\mathfrak{C}_\rho(J)$ but is merely a linear transformation carrying products $x \cdot y$ into $y \cdot x$. It is an anti-*isomorphism* of $\mathfrak{C}_\rho(J)$ and the isotopic algebra $\mathfrak{C}_\kappa(J)$.

3. Algebras with a unity quantity. Let $\mathfrak{C}$ have a unity quantity e so that $e(eJ) = eJ$. Every product $x(xJ)$ is J-symmetric and thus[4] $eJ = e$. It follows that

$$e \cdot x = e(xJ) = xJ = (eJ)(xJ) = [e, x] \tag{6}$$

for every x of $\mathfrak{C}$.

If $\mathfrak{B}$ is an ideal of $\mathfrak{C}_\rho$ or of $\mathfrak{C}_{\kappa\rho}$ the products of its quantities with e are in $\mathfrak{B}$. But then (6) implies that if x is in $\mathfrak{B}$ so is xJ, $\mathfrak{B} = \mathfrak{B}J$. If y is in $\mathfrak{C}$ and x is in $\mathfrak{B}$ the product $x \cdot yJ = xy$ is in $\mathfrak{B}$, $y \cdot xJ = yx$ is in $\mathfrak{B}$, the space $\mathfrak{B}$ is an ideal of $\mathfrak{C}$. Similarly $[xJ, yJ] = xy$, $[yJ, xJ] = yx$ and if $\mathfrak{B}$ is an ideal of $\mathfrak{C}_{\kappa\rho}$ it is an ideal of $\mathfrak{C}$. Conversely if $\mathfrak{B} = \mathfrak{B}J$ is an ideal of $\mathfrak{C}$ the products $x \cdot y$, $y \cdot x$, $[x, y]$, $[y, x]$ are in $\mathfrak{B}$ for every x of $\mathfrak{B}$ and y of $\mathfrak{C}$, $\mathfrak{B}$ is an ideal of $\mathfrak{C}_\rho$, $\mathfrak{C}_{\kappa\rho}$. We have proved

THEOREM 2. *Let $\mathfrak{C}$ be a J-involutorial algebra with a unity quantity. Then a linear subspace $\mathfrak{B}$ of $\mathfrak{C}$ forms an ideal of $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ if and only if $\mathfrak{B} = \mathfrak{B}J$ is an ideal of $\mathfrak{C}$.*

As an immediate consequence we have

THEOREM 3. *Let $\mathfrak{C}$ be a J-involutorial simple algebra with a unity quantity. Then the algebras $\mathfrak{C}_\rho(J)$, $\mathfrak{C}_\kappa(J)$, $\mathfrak{C}_{\kappa\rho}(J)$ are simple.*[5]

---

[3] The transformation J is an anti-automorphism of $C_{\kappa\rho}$. For

$$[x, y]J = \{(xJ)(yJ)\}J = yx = \{(yJ)J\}\{(xJ)J\} = [yJ, xJ].$$

[4] If $\mathfrak{C}$ is an algebra of matrices and r is the maximum rank of any quantity a of $\mathfrak{C}$ then $ea = a$ so that e must have rank r. See Theorem 12 for algebras which then necessarily contain a symmetric idempotent of maximum rank.

[5] If $\mathfrak{A}$ is any central simple algebra and $\mathfrak{A}_0$ is isotopic to $\mathfrak{A}$ it is simple. For $R_x^{(0)} = PR_{xQ}$, $L_x^{(0)} = QL_{xP}$ and if e is the unity quantity of $\mathfrak{A}$ we have $R_f^{(0)} = P$, $L_g^{(0)} = Q$, $f = eQ^{-1}$, $g = eP^{-1}$. Then $T(\mathfrak{A}_0)$ contains P, Q and R_{xQ}, L_{xP} and $T(\mathfrak{A}_0)$ contains $T(\mathfrak{A})$. But if $\mathfrak{A}$ is central simple $T(\mathfrak{A})$ is the algebra of all linear transformations on $\mathfrak{A}$ and contains $T(\mathfrak{A}_0)$, $T(\mathfrak{A}) = T(\mathfrak{A}_0)$, $\mathfrak{A}_0$ is central simple. This result seems to have been observed first by R. H. Bruck. It implies Theorem 3 for central simple algebras.

COROLLARY. *Let $\mathfrak{C}$ be an associative J-involutorial simple algebra. Then $\mathfrak{C}_\rho(J)$, $\mathfrak{C}_\kappa(J)$, $\mathfrak{C}_{\kappa\rho}(J)$ are simple.*

4. Semi-simple algebras. The converse of Theorem 3 is not true and indeed we may prove

THEOREM 4. *Let $\mathfrak{C} = \mathfrak{S} \oplus \mathfrak{S}J$ be a J-involutorial algebra such that S is a simple algebra with a unity quantity. Then $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ are simple.*

For $\mathfrak{C}$ has a unity quantity and every ideal $\mathfrak{B}$ of $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$ or $\mathfrak{C}_{\kappa\rho}$ has the property that $\mathfrak{B} = \mathfrak{B}J$ is an ideal of $\mathfrak{C}$. The non-zero ideals of $\mathfrak{C}$ are $\mathfrak{S}$, $\mathfrak{S}J$, $\mathfrak{C}$ and the only one of these equal to the transformed space under J is $\mathfrak{C}$. Hence $\mathfrak{B} = 0$, $\mathfrak{C}$, the algebras are simple.

Consider any J-involutorial semi-simple algebra $\mathfrak{C}$ with a unity quantity. Then $\mathfrak{C} = \mathfrak{S}_1 \oplus \cdots \oplus \mathfrak{S}_r$ for simple components $\mathfrak{S}_i$ unique apart from their order in the sum. But $\mathfrak{C}J = \mathfrak{S}_1J \oplus \cdots \oplus \mathfrak{S}_rJ = \mathfrak{C}$ and each $\mathfrak{S}_jJ = \mathfrak{S}_i$ for some i. Hence either $\mathfrak{S}_i = \mathfrak{S}_iJ$ or $\mathfrak{S}_i \oplus \mathfrak{S}_iJ$ is a component of $\mathfrak{C}$. Thus we may write $\mathfrak{C} = \mathfrak{B}_1 \oplus \cdots \mathfrak{B}_s$ for components $\mathfrak{B}_j = \mathfrak{B}_jJ$ which are either simple or direct sums as in Theorem 4. Then the $\mathfrak{B}_j$ define simple algebras $(\mathfrak{B}_j)_\rho$, $(\mathfrak{B}_j)_{\kappa\rho}$. Moreover $b_ib_j = b_jb_i = 0$ for every b_i in $\mathfrak{B}_i$ and b_j in $\mathfrak{B}_j \neq \mathfrak{B}_i$. Since $\mathfrak{B}_i = \mathfrak{B}_iJ$, $\mathfrak{B}_j = \mathfrak{B}_jJ$ we have $b_i \cdot b_j = b_j \cdot b_i = [b_i, b_j] = [b_j, b_i] = 0$ and $\mathfrak{C}_\rho$ is the direct sum of its simple components $(\mathfrak{B}_j)_\rho$, $\mathfrak{C}_{\kappa\rho}$ is the direct sum of its simple components $(\mathfrak{B}_j)_{\kappa\rho}$. We have proved that $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ are semi-simple.

Conversely let $\mathfrak{A} = \mathfrak{C}_\rho$ or $\mathfrak{C}_{\kappa\rho}$ be semi-simple so that by Theorem 2 if $\mathfrak{C}$ has a unity quantity the components $\mathfrak{B}_i$ of $\mathfrak{A}$ are r linear subspaces of $\mathfrak{C}$ which are ideals $\mathfrak{B}_i = \mathfrak{B}_iJ$ of $\mathfrak{C}$, $\mathfrak{C} = \mathfrak{B}_1 \oplus \cdots \oplus \mathfrak{B}_r$, $\mathfrak{C}_\rho = (\mathfrak{B}_1)_\rho \oplus \cdots \oplus (\mathfrak{B}_r)_\rho$, $\mathfrak{C}_{\kappa\rho} = (\mathfrak{B}_1)_{\kappa\rho} \oplus \cdots \oplus (\mathfrak{B}_r)_{\kappa\rho}$. The components $\mathfrak{B}_i$ all have unity quantities and $\mathfrak{C}$ will have been proved to be semi-simple when we have proved the following

LEMMA. *Let $\mathfrak{C}$ have a unity quantity and $\mathfrak{C}_\rho$ or $\mathfrak{C}_{\kappa\rho}$ be simple. Then $\mathfrak{C}$ is semi-simple and is either simple or a direct sum $\mathfrak{S} \oplus \mathfrak{S}J$ where $\mathfrak{S}$ is simple.*

We shall be unable to complete the proof of this lemma without a consideration of the radical of an algebra and so we pass on to this study.

5. The radical. The radical of an algebra $\mathfrak{C}$ which is homomorphic to a semi-simple algebra is defined to be [6] the intersection $\mathfrak{R}$ of all ideals $\mathfrak{B}$ of $\mathfrak{C}$

[6] See my paper, "On the radical of a non-associative algebra," *Bulletin of the American Mathematical Society*, vol. 48 (1942), pp. 891-897.

such that $\mathfrak{C} - \mathfrak{B}$ is semi-simple. If $\mathfrak{C}$ is not homomorphic to a semi-simple algebra its radical $\mathfrak{N}$ is the intersection of all ideals $\mathfrak{B}$ of $\mathfrak{C}$ such that $\mathfrak{C} - \mathfrak{B}$ is a zero algebra.

Let S be any automorphism or anti-automorphism of $\mathfrak{C}$. Then S carries $\mathfrak{N}$ into a subspace $\mathfrak{N}S$ of $\mathfrak{C}$. Evidently $\mathfrak{N}S$ is an ideal of $\mathfrak{C}S = \mathfrak{C}$ and $\mathfrak{C}S - \mathfrak{N}S = \mathfrak{C} - \mathfrak{N}\mathfrak{S}$ is semi-simple or a zero algebra according as $\mathfrak{C} - \mathfrak{N}$ is semi-simple or a zero algebra. By the definition of $\mathfrak{N}$ the set $\mathfrak{N}S$ contains $\mathfrak{N}$. The order of $\mathfrak{N}S$ cannot be greater than that of $\mathfrak{N}$, $\mathfrak{N}S = \mathfrak{N}$. The corresponence S induces a correspondence S_0:

$$[x] \to [x]S_0 = [xS]$$

in $\mathfrak{C} - \mathfrak{N}$. If $[x]S_0 = [y]S_0$ then $[xS - yS] = 0$, $(x - y)S$ is in $\mathfrak{N}$ so is $x - y$, $[x] = [y]$. Hence S_0 is a one to one correspondence. Thus it is clear that S_0 is an automorphism, anti-automorphism, or involution of $\mathfrak{C} - \mathfrak{N}$ according as S is an automorphism, anti-automorphism, or involution of $\mathfrak{C}$. We shall use this result only in the case where $S = J$ is an involution and shall prove

THEOREM 5. *Let $\mathfrak{N} \neq 0$ be the radical of a J-involutorial algebra $\mathfrak{C}$. Then $\mathfrak{N} = \mathfrak{N}J$, the algebras $\mathfrak{N}_\rho$, $\mathfrak{N}_\kappa$, $\mathfrak{N}_{\kappa\rho}$ are ideals of $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ respectively such that*

$$(7)\quad (\mathfrak{C} - \mathfrak{N})_\rho = \mathfrak{C}_\rho - \mathfrak{N}_\rho, \quad (\mathfrak{C} - \mathfrak{N})_\kappa = \mathfrak{C}_\kappa - \mathfrak{N}_\kappa, \quad (\mathfrak{C} - \mathfrak{N})_{\kappa\rho} = \mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}.$$

Moreover if $\mathfrak{C} - \mathfrak{N}$ has a unity quantity the algebras $\mathfrak{C}_\rho - \mathfrak{N}_\rho$, $\mathfrak{C}_\kappa - \mathfrak{N}_\kappa$, $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are semi-simple; if $\mathfrak{C} - \mathfrak{N}$ is a zero algebra these algebras are zero algebras.

For we have seen that $\mathfrak{N} = \mathfrak{N}J$, the algebras $\mathfrak{N}_\rho$, $\mathfrak{N}_{\kappa\rho}$ are defined. By the proof of Theorem 2 they are ideals of $\mathfrak{C}_\rho$, $\mathfrak{C}_{\kappa\rho}$ respectively. The linear spaces $\mathfrak{C}$, $\mathfrak{C}_\rho$, $\mathfrak{C}_{\kappa\rho}$ coincide and so do $\mathfrak{N}$, $\mathfrak{N}_\rho$, $\mathfrak{N}_{\kappa\rho}$. Thus the difference groups $\mathfrak{C} - \mathfrak{N}$, $\mathfrak{C}_\rho - \mathfrak{N}_\rho$, $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are the same spaces. But if we define $[x]J_0 = [xJ]$ then multiplication in $(\mathfrak{C} - \mathfrak{N})_\rho$ is defined by $[x] \cdot [y] = [x]\{[y]J_0\} = [x][yJ] = [x(yJ)] = [x \cdot y]$ and this is the product in $\mathfrak{C}_\rho - \mathfrak{N}_\rho$. Similarly the product in $(\mathfrak{C} - \mathfrak{N})_{\kappa\rho}$ is that in $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$. This gives (7). If $\mathfrak{C} - \mathfrak{N}$ has a unity quantity it cannot be a zero algebra and is semi-simple. Then $(\mathfrak{C} - \mathfrak{N})_\rho$ and $(\mathfrak{C} - \mathfrak{N})_{\kappa\rho}$ have already been found to be semi-simple, our result follows from (7). Finally if $\mathfrak{C} - \mathfrak{N}$ is a zero algebra the products $[x] \cdot [y] = [x(yJ)] = [x][yJ] = 0$. Hence $\mathfrak{C}_\rho - \mathfrak{N}_\rho$ and similarly $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are zero algebras.

We may now prove our lemma. Let $\mathfrak{C}_\rho$ or $\mathfrak{C}_{\kappa\rho}$ be simple and $\mathfrak{N}$ be the radical of $\mathfrak{C}$. By Theorem 5 we have $\mathfrak{N} = \mathfrak{N}J$, $\mathfrak{N}_\rho$ is an ideal of $\mathfrak{C}_\rho$, $\mathfrak{N}_{\kappa\rho}$ is an ideal of $\mathfrak{C}_{\kappa\rho}$. But $\mathfrak{N}$ is a proper ideal of $\mathfrak{C}$, the only proper ideal of a simple algebra is zero. Thus $\mathfrak{N} = 0$, $\mathfrak{C}$ has a unity quantity and is not a zero algebra, $\mathfrak{C}$ is semi-simple. The simple components of $\mathfrak{C}$ define simple components $\mathfrak{S} = \mathfrak{S}J$ of $\mathfrak{C}_\rho$ and $\mathfrak{C}_{\kappa\rho}$ or simple components $\mathfrak{S} \oplus \mathfrak{S}J$ of $\mathfrak{C}_\rho$ and $\mathfrak{C}_{\kappa\rho}$. But then $\mathfrak{C} = \mathfrak{S}$ or $\mathfrak{S} \oplus \mathfrak{S}J$. We have proved the first part of

THEOREM 6. *Let $\mathfrak{C}$ be a J-involutorial algebra with a unity quantity. Then $\mathfrak{C}$ is semi-simple if and only if the algebras $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ are all semi-simple. If $\mathfrak{C}$ is not semi-simple and $\mathfrak{N}$ is its radical the algebras $\mathfrak{N}_\rho$, $\mathfrak{N}_\kappa$, $\mathfrak{N}_{\kappa\rho}$ are the respective radicals of $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ and the difference algebras $\mathfrak{C} - \mathfrak{N}$, $\mathfrak{C}_\rho - \mathfrak{N}_\rho$, $\mathfrak{C}_\kappa - \mathfrak{N}_\kappa$, $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are all semi-simple.*

To prove the last part of this theorem we note that $\mathfrak{C}$ is homomorphic to $\mathfrak{C} - \mathfrak{N}$ and thus $\mathfrak{C} - \mathfrak{N}$ has a unity quantity, the algebras $\mathfrak{C}_\rho - \mathfrak{N}_\rho$, $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are semi-simple. Every ideal of $\mathfrak{C}_\rho$ is an algebra $\mathfrak{B}_\rho$ where $\mathfrak{B}$ is an ideal of $\mathfrak{C}$. If $\mathfrak{B}_\rho$ is the radical of $\mathfrak{C}_\rho$ it is contained in $\mathfrak{N}_\rho$ and $\mathfrak{C} - \mathfrak{B}$ is semi-simple. As in the proof of Theorem 5 we have $\mathfrak{C}_\rho - \mathfrak{B}_\rho = (\mathfrak{C} - \mathfrak{B})_\rho$ and by the first part of our theorem $\mathfrak{C} - \mathfrak{B}$ is semi-simple, $\mathfrak{B}$ contains $\mathfrak{N}$. Hence $\mathfrak{B} = \mathfrak{N}$. Similarly $\mathfrak{N}_{\kappa\rho}$ is the radical of $\mathfrak{C}_{\kappa\rho}$.

In the case where $\mathfrak{C}$ is associative we may derive these results without the hypothesis that $\mathfrak{C}$ has a unity quantity. We first have the

LEMMA. *Let $\mathfrak{C}$ be any nilpotent algebra. Then $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ are nilpotent.*

For every product of r factors in either $\mathfrak{C}_\rho$ or $\mathfrak{C}_{\kappa\rho}$ may be expressed as a product of r factors in $\mathfrak{C}$ and is zero if $\mathfrak{C}$ has this property.

We next prove

THEOREM 7. *Let $\mathfrak{C}$ be a J-involutorial associative algebra. Then $\mathfrak{C}$ is semi-simple if and only if $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ are all semi-simple. If $\mathfrak{N} \neq 0$ is the radical of $\mathfrak{C}$ we have $\mathfrak{N} = \mathfrak{N}J$ and $\mathfrak{N}_\rho$, $\mathfrak{N}_\kappa$, $\mathfrak{N}_{\kappa\rho}$ are nilpotent and are the radicals of $\mathfrak{C}_\rho$, $\mathfrak{C}_\kappa$, $\mathfrak{C}_{\kappa\rho}$ respectively, the algebras $\mathfrak{C} - \mathfrak{N}$, $\mathfrak{C}_\rho - \mathfrak{N}_\rho$, $\mathfrak{C}_\kappa - \mathfrak{N}_\kappa$, $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are semi-simple.*

For if $\mathfrak{C}$ is semi-simple it has a unity quantity and $\mathfrak{C}_\rho$ and $\mathfrak{C}_{\kappa\rho}$ are semi-simple. Conversely let $\mathfrak{N}$ be the radical of $\mathfrak{C}$. Then we have seen that $\mathfrak{N} = \mathfrak{N}J$ and that $\mathfrak{N}_\rho$ *contains* the radical of $\mathfrak{C}_\rho$, $\mathfrak{N}_{\kappa\rho}$ of $\mathfrak{C}_{\kappa\rho}$. For $\mathfrak{C} - \mathfrak{N}$ is a semi-simple algebra with a unity quantity, $\mathfrak{C}_\rho - \mathfrak{N}_\rho$ and $\mathfrak{C}_{\kappa\rho} - \mathfrak{N}_{\kappa\rho}$ are semi-simple. If $\mathfrak{C}_\rho$ or $\mathfrak{C}_{\kappa\rho}$ is semi-simple its ideals are semi-simple whereas

$\mathfrak{R}_\rho$, $\mathfrak{R}_{\kappa\rho}$ are zero or nilpotent ideals. Hence $\mathfrak{R} = 0$, $\mathfrak{C}$ is semi-simple. If neither $\mathfrak{C}$, $\mathfrak{C}_\rho$ nor $\mathfrak{C}_{\kappa\rho}$ is semi-simple and $\mathfrak{B}$ is the radical of $\mathfrak{C}_\rho$ then $\mathfrak{C}_\rho - \mathfrak{R}_\rho$ is semi-simple, $\mathfrak{B}$ is contained in $\mathfrak{R}_\rho$, $\mathfrak{C} - \mathfrak{B}$ is semi-simple. But $\mathfrak{R}_\rho - \mathfrak{B}$ is zero or a nilpotent ideal of the semi-simple algebra $\mathfrak{C}_\rho - \mathfrak{B}$, $\mathfrak{R}_\rho - \mathfrak{B} = 0$, $\mathfrak{B} = \mathfrak{R}_\rho$. Similarly $\mathfrak{R}_{\kappa\rho}$ is the radical of $\mathfrak{C}_{\kappa\rho}$.

It should be noted that the results of this theorem depend only on the property that the radical of $\mathfrak{C}$ is nilpotent and that when $\mathfrak{C}$ is semi-simple it has a unity quantity. Hence they hold also under the weaker hypothesis that $\mathfrak{C}$ is an alternative algebra rather than an associative algebra.

6. Row algebras. We shall begin our study of subalgebras of $\mathfrak{C}_\rho$ by exhibiting certain revealing examples of such algebras. We first suppose that $\mathfrak{G}$ is any algebra whatever and $a \to aS$ is an anti-isomorphism of $\mathfrak{G}$ on an algebra which we shall designate by $\mathfrak{G}\mathfrak{S}$. Construct the direct sum $\mathfrak{C} = \mathfrak{G} \oplus \mathfrak{G}S$ and define $(c_1 + c_2S)J = c_1S + c_2$ for every c_1 of $\mathfrak{G}$ and c_2 of $\mathfrak{G}S$. Then J is an involution of $\mathfrak{C}$. However $c_1 \cdot c_2 = c_1(c_2S) = 0$ for every c_1 and c_2 of $\mathfrak{G}$. It follows that $\mathfrak{G}$ forms a subalgebra $\mathfrak{A}$ of $\mathfrak{C}_\rho$ which is a zero algebra. However $\mathfrak{G} \neq \mathfrak{G}J$, $\mathfrak{A} \neq \mathfrak{B}_\rho$ for a subalgebra $\mathfrak{B}$ of $\mathfrak{C}$. Nevertheless the space $\mathfrak{G}$ is a subalgebra of $\mathfrak{C}$.

We next suppose that $\mathfrak{C}$ is the set of all $2n$-rowed square matrices and that J is the transformation $x \to xJ = x'$ of transposition. We let $\mathfrak{M}$ be the set of all matrices of the form

$$a = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

for A an n-rowed square matrix, and

$$e = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}, \quad eJ = \begin{pmatrix} 0 & 0 \\ I & 0 \end{pmatrix}, \quad e(eJ) = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix},$$

where I is the identity matrix of n rows. Then $\mathfrak{M}$ is a subalgebra of $\mathfrak{C}$, $\mathfrak{M}$ is simple, $f = e \cdot e = e(eJ)$ is the unity quantity of $\mathfrak{M}$. Also

$$a \cdot e = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ I & 0 \end{pmatrix} = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\begin{pmatrix} A' & 0 \\ 0 & 0 \end{pmatrix} = e \cdot a = 0.$$

We define $\mathfrak{A}$ as the linear subspace

$$\mathfrak{A} = \mathfrak{M} + e\mathfrak{F}$$

of $\mathfrak{C}$. Then $\mathfrak{A}$ has order $n^2 + 1$ and since $\mathfrak{M} = \mathfrak{M}J$ and $e \neq eJ$ the set

$\mathfrak{A} \neq \mathfrak{A}J = \mathfrak{M} + (eJ)\mathfrak{F}$. Moreover if a and b are in $\mathfrak{M}$ and α and β are in $\mathfrak{F}$ we have

$$(a + \alpha e) \cdot (b + \beta e) = a \cdot b + \alpha\beta e$$

is in $\mathfrak{M}$. It follows that $\mathfrak{A}$ is a row algebra. However if $\mathfrak{A}$ is a non-scalar matrix the product

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$$

is not in $\mathfrak{A}$ and $\mathfrak{A}$ is not a subalgebra of $\mathfrak{C}$, $\mathfrak{A} \neq \mathfrak{D}_\rho$ for any subalgebra $\mathfrak{D} = \mathfrak{D}J$ of $\mathfrak{C}$.

The subspace $\mathfrak{M} = \mathfrak{M}J$ defines a subalgebra $\mathfrak{M}_\rho$ of $\mathfrak{A}$. Also $\mathfrak{M}_\rho{\cdot}^2 = \mathfrak{M}_\rho$ since $\mathfrak{M} = \mathfrak{M}J$ is simple. But $\mathfrak{A}{\cdot}^2 \leq \mathfrak{M}_\rho$, $\mathfrak{A}{\cdot}^2 = \mathfrak{M}_\rho$. Let $\mathfrak{B}$ be any other non-zero ideal of $\mathfrak{A}$. Then $\mathfrak{B} \leq \mathfrak{M}_\rho$ implies that $\mathfrak{B} = \mathfrak{M}_\rho$. Hence $\mathfrak{B}$ contains a quantity $a + \alpha e$ with a in $\mathfrak{M}$ and $\alpha \neq 0$. But $(a + \alpha e) \cdot (\alpha^{-1}e) = f$ is in $\mathfrak{B}$ and $\mathfrak{B}$ contains $\mathfrak{M}$, $\mathfrak{B}$ contains $(a + \alpha e) - a = \alpha e$, $\mathfrak{B} = \mathfrak{A}$. Hence $\mathfrak{A}$ and $\mathfrak{M}_\rho$ are the only non-zero ideals of $\mathfrak{A}$. Since $\mathfrak{A}$ is not semi-simple its radical is $\mathfrak{M}_\rho = \mathfrak{A}{\cdot}^2$, $\mathfrak{A} - \mathfrak{M} = \mathfrak{A} - \mathfrak{A}{\cdot}^2$ is a zero algebra.

Our final algebra is the direct sum $\mathfrak{B} = \mathfrak{S} \oplus \mathfrak{A}$ where $\mathfrak{A}$ is the algebra above and $\mathfrak{S} = \mathfrak{M}_{0\rho}$ for a total matric algebra $\mathfrak{M}_0$. Thus $\mathfrak{S}$ consists of all $3n$-rowed square matrices

$$\begin{pmatrix} A & xe & 0 \\ 0 & 0 & 0 \\ 0 & 0 & B \end{pmatrix}.$$

As before $\mathfrak{S} = \mathfrak{S}J$, $\mathfrak{B} \neq \mathfrak{A}J$, $\mathfrak{B} \neq \mathfrak{D}_\rho$ for any subalgebra $\mathfrak{D} = \mathfrak{D}J$ of the set $\mathfrak{C}$ of all $3n$-rowed square matrices. But $\mathfrak{B}$ is a row algebra.

The ideal $\mathfrak{M}_\rho$ of $\mathfrak{A}$ is one ideal of $\mathfrak{B}$, $\mathfrak{A}$ is an ideal of $\mathfrak{B}$, $\mathfrak{S}$ is an ideal of $\mathfrak{B}$. These are the only ideals of $\mathfrak{B}$ contained in either $\mathfrak{A}$ or $\mathfrak{S}$. Let $\mathfrak{L} \neq 0$ be any ideal of $\mathfrak{B}$ not contained in $\mathfrak{A}$ or in $\mathfrak{S}$. Then $\mathfrak{L}$ contains a quantity $z + a$ where $z \neq 0$ is in $\mathfrak{S}$ and $a \neq 0$ is in $\mathfrak{A}$. But if g is the unity quantity of $\mathfrak{M}_0$ we have $(z + a) \cdot g = zg + ag = zg = z \neq 0$ is in $\mathfrak{M}_0$. Now this product is in $\mathfrak{L}$ and so is $y \cdot [xJ \cdot z] = y[(xJ)(zJ)] = y(zx)$ for every y and x of $\mathfrak{M}_0$. Since $\mathfrak{M}_0$ is simple $\mathfrak{L}$ contains $\mathfrak{M}_0$. Hence $\mathfrak{L} = \mathfrak{S} \oplus \mathfrak{L}_0$ where $\mathfrak{L}_0$ is a subspace of $\mathfrak{A}$. Clearly $\mathfrak{L}_0$ is an ideal of $\mathfrak{A}$, $\mathfrak{L}_0 = \mathfrak{A}$ or $\mathfrak{M}_\rho$, $\mathfrak{L} = \mathfrak{S} + \mathfrak{A}$ or $\mathfrak{B}$.

The algebra $\mathfrak{B}$ is homomorphic to $\mathfrak{B} - (\mathfrak{S} + \mathfrak{M}_\rho) = \mathfrak{A} - \mathfrak{M}_\rho$ and is not semi-simple. The only other difference algebras to which $\mathfrak{B}$ is homomorphic are $\mathfrak{B} - \mathfrak{S} \cong \mathfrak{A}$, $\mathfrak{B} - \mathfrak{A} \cong \mathfrak{S}$, $\mathfrak{B} - \mathfrak{M}_\rho \cong \mathfrak{S} \oplus (\mathfrak{A} - \mathfrak{M}_\rho)$ and of these only $\mathfrak{B} - \mathfrak{A}$ is semi-simple. Hence $\mathfrak{A}$ *is the radical of* $\mathfrak{B}$. It follows that the radical $\mathfrak{N}$ of a row algebra $\mathfrak{B}$ need not have the property $\mathfrak{N} = \mathfrak{N}J$.

We have now seen that if $\mathfrak{A}$ is a row algebra neither $\mathfrak{A}$ nor its radical need have the property $\mathfrak{A} = \mathfrak{A}J$. Thus this property is a consequence only of additional hypotheses. It is a most important property since it implies that $x \cdot yJ = xy$ is in $\mathfrak{A}$, $\mathfrak{A} = \mathfrak{D}_\rho$ for a subalgebra $\mathfrak{D}$ of $\mathfrak{C}$. Let us now prove

THEOREM 8. *If $\mathfrak{A}$ is a row algebra its ideal $\mathfrak{A}^{\cdot 2} = (\mathfrak{A}^{\cdot 2})J$ and has the property $\mathfrak{A}^{\cdot 2} = \mathfrak{D}_\rho$ for a subalgebra $\mathfrak{D}$ of $\mathfrak{C}$.*

For $(x \cdot y)J = y \cdot x$ is in $\mathfrak{A}^{\cdot 2}$ for every x and y of $\mathfrak{A}$, $(\mathfrak{A}^{\cdot 2})J$ is contained in $\mathfrak{A}^{\cdot 2}$. Since $J^2 = I$ we have $\mathfrak{A}^{\cdot 2} = (\mathfrak{A}^{\cdot 2})J$.

We have the immediate consequences

COROLLARY I. *Let $\mathfrak{A} = \mathfrak{A}^{\cdot 2}$ be a row algebra. Then $\mathfrak{A} = \mathfrak{A}J = \mathfrak{D}_\rho$ for a subalgebra $\mathfrak{D}$ of $\mathfrak{C}$.*

COROLLARY II. *Every semi-simple row algebra $\mathfrak{A}$ is an algebra $\mathfrak{D}_\rho$ where $\mathfrak{D}$ is a semi-simple subalgebra of $\mathfrak{C}$ and $\mathfrak{A}$ is isotopic to $\mathfrak{D}$.*

COROLLARY III. *Let $\mathfrak{C}$ be associative and $\mathfrak{A}$ be a semi-simple row algebra Then $\mathfrak{A}$ is isotopic to an associative semi-simple algebra $\mathfrak{D}$, $\mathfrak{A} = \mathfrak{D}_\rho$.*

For row algebras in which $\mathfrak{A}$ may not be equal to $\mathfrak{A}^{\cdot 2}$ we may prove

THEOREM 9. *Let a row algebra $\mathfrak{A}$ be homomorphic to some semi-simple algebra, $\mathfrak{N}$ be the radical of $\mathfrak{A}$, $\mathfrak{G}$ be the set of all quantities x of $\mathfrak{A}$ such that xJ is in $\mathfrak{A}$, $\mathfrak{N}_0$ be the intersection of $\mathfrak{N}$ and $\mathfrak{G}$ so that $\mathfrak{N} = \mathfrak{N}_0 + \mathfrak{N}_1$. Then*

$$\mathfrak{A} = \mathfrak{G} + \mathfrak{N}_1,$$

$\mathfrak{G}$ is an ideal of $\mathfrak{A}$ containing $\mathfrak{A}^{\cdot 2}$, $\mathfrak{A} - \mathfrak{G}$ is a zero algebra. Moreover $\mathfrak{N}_0$ is an ideal of $\mathfrak{A}$ and of $\mathfrak{G}$ such that

$$\mathfrak{A} - \mathfrak{N} \cong \mathfrak{G} - \mathfrak{N}_0.$$

For by Theorem 8 we have $\mathfrak{A}^{\cdot 2} = (\mathfrak{A}^{\cdot 2})J$, $\mathfrak{G}$ contains $\mathfrak{A}^{\cdot 2}$ and thus $\mathfrak{A}\mathfrak{G}$ and $\mathfrak{G}\mathfrak{A}$. Hence $\mathfrak{G}$ is an ideal of $\mathfrak{A}$ and $\mathfrak{A} - \mathfrak{G}$ is a zero algebra. Since both $\mathfrak{N}$ and $\mathfrak{G}$ contain $\mathfrak{A}\mathfrak{N}$ and $\mathfrak{N}\mathfrak{A}$ their intersection $\mathfrak{N}_0$ contains $\mathfrak{A}\mathfrak{N}_0$ and $\mathfrak{N}_0\mathfrak{A}$, $\mathfrak{N}_0$ is an ideal of $\mathfrak{A}$ and of $\mathfrak{G}$. The algebra $\mathfrak{A} - \mathfrak{N}$ is semi-simple, $\mathfrak{A} - \mathfrak{N} = (\mathfrak{A} - \mathfrak{N})^{\cdot 2}$ is an algebra whose quantities are sums of products $[a][x] = [a \cdot x] = [b]$ where b is in $\mathfrak{G}$. But then every quantity of $\mathfrak{A}$ has the form $b + f$ where b is in $\mathfrak{G}$ and f is in $\mathfrak{N}$, we may take f in $\mathfrak{N}_1$, $\mathfrak{A} = \mathfrak{G} + \mathfrak{N}_1$. If $[b] = [b_1]$ where b and b_1 are in $\mathfrak{G}$ then $b - b_1$ is in $\mathfrak{N}$ and in $\mathfrak{G}$, $b - b_1$ is

in $\mathfrak{N}_0$. Thus the mapping $[b] \to b$ of the classes $[b]$ of $\mathfrak{A} - \mathfrak{N}$ on the classes $\{b\}$ of $\mathfrak{G} - \mathfrak{N}_0$ is one to one and defines an equivalence of these algebras.

In the example we have given of such an algebra the algebra $\mathfrak{G}$ is semi-simple but $\mathfrak{N}_0$ is not zero. Thus $\mathfrak{N}_0$ contains the radical of $\mathfrak{G}$ and may contain it properly.

In closing this part of our discussion let us observe that if a is the n-rowed square matrix with unity in the first row and second column and zeros elsewhere and if J is transposition then $[a, a] = (aJ)(aJ) = 0$. Then a spans a linear space $\mathfrak{A}$ of order one such that $\mathfrak{A} \neq \mathfrak{A}J$, $\mathfrak{A}$ is a column by row algebra and is actually a zero algebra. We also note that if $\mathfrak{A}$ is any column by row algebra then the set $\mathfrak{B}$ of all quantities x of $\mathfrak{A}$ such that xJ is in $\mathfrak{A}$ is a sub-algebra of $\mathfrak{A}$, $\mathfrak{B} = \mathfrak{D}_{\kappa\rho}$. For if x and y are in $\mathfrak{B}$ so are xJ and yJ, $[x, y]J = [yJ, xJ]$ is in $\mathfrak{A}$, $[x, y]$ is in $\mathfrak{B}$. However it does not seem likely that $\mathfrak{B}$ is an ideal of $\mathfrak{A}$ nor that any results like those derived above for row algebras are obtainable.

7. Real algebras. A field $\mathfrak{F}$ is said to be real if no sum of a finite number of non-zero squares of its quantities is zero. If A is any matrix and A' is its transpose the i-th diagonal element of $B = AA'$ is the sum of the squares of the quantities in the i-th row of A. If A has rank r the symmetric matrix B has rank at most r and is congruent to a diagonal matrix $PBP' = (PA)(PA)'$ where P is non-singular. But PA has rank r and at least r non-zero rows, PBP' has at least r non-zero diagonal elements. Thus the rank of PBP' and of B is at least r, AA' has rank r. It follows very simply that *a field F is real if and only if the rank of every matrix A coincides with the rank of AA'.* We now note the known [7]

LEMMA. *Let $\mathfrak{C}$ be an algebra over a real field $\mathfrak{F}$ of n-rowed square matrices under ordinary matrix multiplication and let the transpose xJ of every matrix x of $\mathfrak{C}$ be in $\mathfrak{C}$. Then $\mathfrak{C}$ is a semi-simple algebra, $\mathfrak{C} = \mathfrak{S}_1 \oplus \cdots \oplus \mathfrak{S}_r$ for simple algebras $\mathfrak{S}_i = \mathfrak{S}_iJ$.*

For we have seen that the radical $\mathfrak{N}$ of the associative algebra $\mathfrak{C}$ has the property $\mathfrak{N} = \mathfrak{N}J$. If $\mathfrak{N} \neq 0$ there is a non-zero matrix x of rank r in $\mathfrak{N}$. Then $y = x(xJ)$ is in $\mathfrak{N}$ and is a nilpotent symmetric matrix of rank r, $y^t = 0$. But $y^r = yy'$ has rank r, y^{2^k} has rank r for every k, k may be chosen so that $2^k > t$, a contradiction. Hence $\mathfrak{N} = 0$, $\mathfrak{C}$ is semi-simple. If $\mathfrak{C}_i$ is the unity

[7] Cf. page 283 of H. Weyl, "On the use of indeterminates in the theory of the orthogonal and symplectic groups," *American Journal of Mathematics*, vol. 63 (1941), pp. 777-784. We shall give a brief proof here of this result for the sake of completeness.

quantity of $\mathfrak{S}_i$ then e_iJ is the unity quantity of $\mathfrak{S}_iJ$ and we have already seen that if $\mathfrak{S}_iJ \neq \mathfrak{S}_i$ then $\mathfrak{S}_iJ$ is in the direct sum relation to $\mathfrak{S}_i$. But then $e_i(e_iJ) = 0$ which is impossible. Hence $\mathfrak{S}_i = \mathfrak{S}_iJ$.

Our final result will be

THEOREM 10. *Let $\mathfrak{A}$ be a linear space of real matrices forming an algebra under row by row multiplication such that $\mathfrak{A}^{\cdot 2} = \mathfrak{A}$. Then $\mathfrak{A}$ contains the transpose xJ of every x of $\mathfrak{A}$, $\mathfrak{A}$ is semi-simple, $\mathfrak{A} = \mathfrak{B}_\rho$ is the isotope of an associative semi-simple algebra $\mathfrak{B} = \mathfrak{S}_1 \oplus \cdots \oplus \mathfrak{S}_r$ for simple components $\mathfrak{S}_i = \mathfrak{S}_iJ$ such that $\mathfrak{A} = (\mathfrak{S}_1)_\rho \oplus \cdots \oplus (\mathfrak{S}_r)_\rho$.*

This result follows from the fact that necessarily $\mathfrak{A} = \mathfrak{B}_\rho$ and that if $\mathfrak{B} = \mathfrak{B}J$ then $\mathfrak{B}$ is semi-simple. It gives a complete construction of all row algebras $\mathfrak{A} = \mathfrak{A}^{\cdot 2}$ as well as of the ideal $\mathfrak{G}$ of Theorem 9 which is now seen to be semi-simple in case $\mathfrak{F}$ is real and J is transposition.

THE UNIVERSITY OF CHICAGO.

ON THE FORMS OF THE PREDICATES IN THE THEORY OF CONSTRUCTIVE ORDINALS.*

By S. C. Kleene.

In the system S_3 of notation for ordinal numbers, the class O of the natural numbers which represent ordinals, and the partial ordering relation $<_O$ between such numbers, were defined by a transfinite induction.[1] In this paper, we shall prove that the predicates $a \epsilon O$ and $a <_O b$ are expressible explicitly in the respective forms $(x)(Ey)R(a, x, y)$ and $(x)(Ey)S(a, b, x, y)$ where R and S are primitive recursive predicates. The result is used elsewhere to exhibit the incompleteness of ordinal logics under a general theorem on recursive predicates and quantifiers.[2] The proof illustrates a technique to which recourse may be had generally in attempts to reduce inductive definitions to explicit ones. Some simpler applications of the technique are given first, as well as a résumé of requisite notions and results.

1. Recursive definition. We shall deal with number-theoretic *functions*, the independent variables of which range over the natural numbers, with the values of the functions being taken from the same domain; and with number-theoretic *predicates*, that is, propositional functions of natural numbers.

Such functions and predicates can be defined in various ways. It often happens that the definition which is given for a function provides a uniform method which would enable one, given any set of arguments, to ascertain the corresponding value of the function in a finite number of steps. Likewise, the definition of a predicate may provide effective means for reaching a decision respecting the truth or falsity of the proposition taken as value of the predicate for a given set of arguments. Under these circumstances, we say that the function or predicate is *constructively* defined.

We shall refer to *primitive recursive* functions and predicates, and to *general recursive* functions and predicates. These are the functions and predicates definable by two particular types of constructive definition which

* Received October 15, 1942; Preliminary report presented to the American Mathematical Society, April 3, 1942. Theorems 1 and 2 were obtained in 1939-40 in progress of research at the Institute for Advanced Study supported by the Institute and the Alumni Research Foundation of the University of Wisconsin. The bracketed numbers refer to the bibliography at the end.

1 [9] p. 155.

2 [10] §§ 5, 15.

have been described elsewhere, the second of which includes the first.[3] From work of Church and Turing, it appears that any function or predicate which is constructively definable is general recursive.[4] This lends the general recursive functions their chief interest, while moreover the cursory reader may use it as a principle in verifying our statements that certain functions and predicates are general recursive. The additional fact that some of them are primitive recursive is incidental for this paper.

2. Explicit definition. After some predicates and functions have been defined, then other predicates can be defined *explicitly* by giving for them expressions of finite length built up, with the use of variable natural numbers, in terms of previously defined predicates and functions, and the operations of logic.

The operations of logic which we shall consider are the *propositional connectives*

$$\vee \text{ (or)}, \quad \& \text{ (and)}, \quad {}^{-} \text{ (not)}, \quad \rightarrow \text{ (implies)},$$

and the *quantifiers*,

$$(Ex) \text{ (there exists an } x \text{ such that)}, \quad (x) \text{ (for all } x).$$

The predicates which can be introduced by explicit definitions, when we use these operations of logic and start from the general recursive predicates and functions as given, including the recursive predicates themselves, the author has called *elementary*.

Explicit definition may also be considered under other restrictions as to the terms.

3. Reduction. It may happen that two distinct definitions introduce predicates which can then be shown to be equivalent. If extensional terminology is used, the definitions are recognized as two definitions of the same predicate; or, in the language of conditions, either one becomes a necessary and sufficient condition for the other.

In the case that the one predicate is expressed explicitly in a certain form or in certain terms only, we shall speak of this relationship as a *reduction* of the other predicate to that form or to those terms; and the other is said to be *expressible* in that form or in those terms.

For example, it is known that every elementary predicate is expressible in terms of the functions $+$ (plus), $\cdot$ (times) and the predicate $=$ (equals),

---

[3] [5] §§ 2, 9, [7] pp. 729-31, [10] §§ 1, 2. [4] [1] § 7, [14], [10] § 12.

and the operations of logic.[5] One can thus get along with these three very simple constructive functions and predicates, at the cost of increasing the numbers of operations of logical combination which will be required to express given predicates in terms of them.

After some preliminaries, we shall describe in **6** a reduction of opposite tendency.

4. Advancement of quantifiers. The following equivalences, where A is independent of x, hold in the classical logic.

$$(1) \qquad (Ex)A(x) \vee (Ex)B(x) \equiv (Ex)(A(x) \vee B(x)),$$
$$(2) \qquad A \vee (Ex)B(x) \equiv (Ex)(A \vee B(x)),$$
$$(3) \qquad A \,\&\, (Ex)B(x) \equiv (Ex)(A \,\&\, B(x)),$$
$$(4^*) \qquad \overline{(Ex)A(x)} \equiv (x)\bar{A}(x),$$
$$(5) \qquad (x)A(x) \,\&\, (x)B(x) \equiv (x)(A(x) \,\&\, B(x)),$$
$$(6) \qquad A \,\&\, (x)B(x) \equiv (x)(A \,\&\, B(x)),$$
$$(7^*) \qquad A \vee (x)B(x) \equiv (x)(A \vee B(x)),$$
$$(8^*) \qquad \overline{(x)A(x)} \equiv (Ex)\bar{A}(x).$$

By applying them from left to right, using as required the associative and commutative laws for $\vee$ and &, we can advance quantifiers in an expression across the connectives $\vee$, & and $^{-}$ toward the front or exterior of the expression. With the classical equivalence

$$(9^*) \qquad A \rightarrow B \equiv \bar{A} \vee B,$$

we can do the same for $\rightarrow$. For example, using (9*) with (2) and (7*), respectively, A being independent of x,

$$(10^*) \qquad A \rightarrow (Ex)B(x) \equiv (Ex)(A \rightarrow B(x)),$$
$$(11^*) \qquad A \rightarrow (x)B(x) \equiv (x)(A \rightarrow B(x)).$$

In the intuitionistic logic, in which the classical law of the excluded middle $A \vee \bar{A}$ is not postulated, the starred equivalences fail to hold in general. However, under special conditions various ones of them hold intuitionistically, as a consequence of the fact that, when A is known to be general recursive, then $A \vee \bar{A}$ can be proved. To begin with, (7*) and (9*) hold intuitionistically, if A is recursive; and hence (10*) and (11*) do. Again, the following form of (7*), A and C being independent of x,

$$(12^*) \qquad (A \,\&\, C) \vee (x)B(x) \equiv (x)((A \,\&\, C) \vee B(x)),$$

[5] [4] pp. 191-3, [6] pp. 412-21, [8].

holds intuitionistically, if A is recursive and A and $B(x)$ are mutually exclusive.

5. Contraction of quantifiers. Let $(x)_i$ denote the exponent of the i-th prime in the representation of x as a product of powers of distinct prime numbers, for x and i positive.[c] This exponent is 0, if the i-th prime does not divide x. For $x = 0$ or $i = 0$, let $(x)_i$ be 0. Then $(x)_i$ is in fact a primitive recursive function of x and i. Moreover,

$$x \neq 0 \rightarrow (x)_i < x. \tag{13}$$

Consider the ordered set of n quantities $(x)_1, \cdots, (x)_n$. This ranges with repetitions over all n-tuples of natural numbers as x ranges over all natural numbers. Therefore

$$(Ex_1) \cdots (Ex_n) A(x_1, \cdots, x_n) \equiv (Ex) A((x)_1, \cdots, (x)_n), \tag{14}$$

$$(x_1) \cdots (x_n) A(x_1, \cdots, x_n) \equiv (x) A((x)_1, \cdots, (x)_n). \tag{15}$$

Indeed, the set $(x)_1, \cdots, (x)_n$ takes on each n-tuple as value for infinitely many values of x. Hence we may exclude any finite number of values from the range of x in (14) and (15). For example, excluding the value 0,

$$(Ex_1) \cdots (Ex_n) A(x_1, \cdots, x_n) \equiv (Ex)[A((x)_1, \cdots, (x)_n) \;\&\; x \neq 0], \tag{16}$$

$$(x_1) \cdots (x_n) A(x_1, \cdots, x_n) \equiv (x)[A((x)_1, \cdots, (x)_n) \vee x = 0]. \tag{17}$$

6. Recursive predicates and quantifiers. Consider any predicate expressed in terms of general recursive predicates and quantifiers only. The expression for the predicate has the form of a recursive predicate with zero or more quantifiers prefixed. By the contraction laws (14) and (15), consecutive occurrences of like quantifiers can be eliminated without altering the recursive character of the operand of the quantifiers. Hence for a predicate of a single variable a only the following normal forms need be considered:

$$R(a) \quad \begin{array}{llll} (Ex)R(a,x) & (x)(Ey)R(a,x,y) & (Ex)(y)(Ez)R(a,x,y,z) & \cdots \\ (x)R(a,x) & (Ex)(y)R(a,x,y) & (x)(Ey)(z)R(a,x,y,z) & \cdots, \end{array}$$

where the R for the form is general recursive; and similarly replacing a by $a_1, \cdots, a_n$ for predicates of n variables $a_1, \cdots, a_n$.

In the classical logic, furthermore, given any expression for an elementary

---

[c] This $(x)_i$ is the $i\,Gl\,x$ of [7] p. 732, which is a modification of the $i\,Gl\,x$ of [4] p. 182.

predicate as described in **2**, the quantifiers can be advanced to the front as described in **4**. By theorems on the composition of recursive predicates with recursive functions and the operations of the propositional calculus, the operand of the prefixed quantifiers after the advancement constitutes a simple recursive predicate.[7] Hence, classically, the normal forms just described suffice for the expression of every elementary predicate.

In this reduction for elementary predicates, the rôle of the logical operations is minimized at the cost of increasing the complexity of the recursive predicates. But if the notion of a given constructive predicate is accepted as clear, then these reduced forms stand out as particularly clear for the interpretation of the predicates.

No further essential reduction in the list of the normal forms is possible, by the theorem of the author which says that, classically, to each of the listed forms after the first, there is a predicate expressible in that form but neither in the dual form nor in any of the forms with fewer quantifiers.[8] The theorem also has an intuitionistic version. In connection with this theorem, the author has shown how a number of questions in the foundations of mathematics turn upon a predicate's being expressible in a certain one or another of these forms.[9]

If a predicate is expressed in one of the forms after the first, then it is always possible to replace the R by another R which is primitive recursive, retaining the form.[10]

7. Inductive definition. *Inductive* definition is most familiar in the case that a class is being defined, but the method applies equally well to predicates of more than one variable. The general features of an inductive definition are these. First, there are *direct* clauses. Some of these (*basic* clauses) state that the predicate is true for certain sets of arguments; others (*inductive* clauses) that if it is true for certain sets of arguments, then it is true for others related in a certain way to the former. Then there is an *extremal* clause, which states that the predicate is true only for those sets of arguments for which its truth is required by the direct clauses. These features are illustrated in the examples to be given presently; and our work will be with the examples.

The direct clauses of an inductive definition may be *constructive* in the sense that any proposed particular application of one of them can be recognized as legal or illegal; or some of them may be non-constructive. When one of the clauses requires as premises for its application the truth of the predicate

[7] [4] I-IV.

[8] [10] § 5.

[9] [10] §§ 11-17.

[10] [10] § 9.

for infinitely many sets of arguments, the inductive definition is *transfinite*.

In this paper we are concerned with the problem of reducing inductive definitions to explicit ones; more specifically, with the problem, to a given inductive definition of a predicate, of finding an equivalent elementary one. By **6**, were such found, then classically we could reduce it to one of the normal forms in terms of recursive predicates and quantifiers. However the technique which we present below for reducing inductive definitions is an extension of that of **6**, and when it succeeds we arrive at the latter directly. As it happens, for our examples, the reduction requires only intuitionistic methods.

8. The concept of formal provability. Inductive definitions of metamathematical predicates occur in the description of a formal deductive system. The predicates become number-theoretic ones when a Gödel arithmetization of metamathematics is applied to the system.[11] Let us consider the arithmetized provability predicate. Suppose that the system has one and two premise rules of inference. We shall then have given three predicates:—$A(a)$: a is an axiom (i. e., a is the Gödel number of an axiom of the unarithmetized formal system); $B(a, b)$: a is an immediate consequence of b by a one premise rule of inference; $C(a, b, c)$: a is an immediate consequence of b and c by a two premise rule of inference. We shall suppose that the predicates A, B and C are general recursive (in effect, that the formal system has constructive rules). The four clauses which follow constitute the inductive definition of the predicate:—$P(a)$: a is provable.

1. If $A(a)$, then $P(a)$. 2. If $P(b)$ and $B(a, b)$, then $P(a)$. 3. If $P(b)$ and $P(c)$ and $C(a, b, c)$, then $P(a)$. 4. $P(a)$ only as required by 1-3.

Rewriting this definition of $P(a)$ in the form of an equivalence, using the logical symbolism,

$$(18)\quad \begin{aligned} P(a) \equiv A(a) \vee (Ex)[P(x) \,\&\, B(a, x)] \\ \vee (Ex)(Ey)[P(x) \,\&\, P(y) \,\&\, C(a, x, y)]. \end{aligned}$$

We now conjecture that $P(a)$ is expressible in the form $(Ex)R(a, x)$ where R is general recursive; and substitute tentatively the expression "$(Ex)R(a, x)$," with "R" representing an as yet undetermined predicate, for "$P(a)$" in (18). Thus, making suitable changes in the bound variables,

$$(19)\quad \begin{aligned} (Ex)R(a, x) \equiv A(a) \vee (Ex)[(Ez)R(x, z) \,\&\, B(a, x)] \\ \vee (Ex)(Ey)[(Ez)R(x, z) \,\&\, (Ez)R(y, z) \,\&\, C(a, x, y)]. \end{aligned}$$

[11] [4], [10] § 4.

Advancing quantifiers to the front by (1)-(3), with a change of notation in the bound variables,

$$(20)\quad (Ex)R(a,x) \equiv (Ex_1)(Ex_2)(Ex_3)(Ex_4)[A(a) \vee [R(x_1,x_2) \,\&\, B(a,x_1)] \vee [R(x_1,x_3) \,\&\, R(x_2,x_4) \,\&\, C(a,x_1,x_2)]].$$

Thence, contracting by (16),

$$(21)\quad (Ex)R(a,x) \equiv (Ex)\{[A(a) \vee [R((x)_1,(x)_2) \,\&\, B(a,(x)_1)] \vee [R((x)_1,(x)_3) \,\&\, R((x)_2,(x)_4) \,\&\, C(a,(x)_1,(x)_2)]] \,\&\, x \neq 0\}.$$

Striking out the prefixed quantifier (Ex) from both members of the last equivalence,

$$(22)\quad R(a,x) \equiv [A(a) \vee [R((x)_1,(x)_2) \,\&\, B(a,(x)_1)] \vee [R((x)_1,(x)_3) \,\&\, R((x)_2,(x)_4) \,\&\, C(a,(x)_1,(x)_2)]] \,\&\, x \neq 0.$$

This equivalence determines $R(a,x)$ as a general recursive predicate, since for $x \neq 0$, $R(a,x)$ is expressed by it in terms of given general recursive predicates and functions, the operations of the propositional calculus, and the predicate $R(s,t)$ itself for only arguments s, t such that $t < x$ by (13), while for $x = 0$, it makes $R(a,x)$ definitely false. That is, we can take this equivalence as the definition of R, and R will then be general recursive. Then if we define P from R by

$$(23)\quad P(a) \equiv (Ex)R(a,x),$$

by reversing the steps from (18) to (22) we can prove (18) as a theorem from (22) and (23) as definitions. But (18) as we know is sufficient to define $P(a)$ as a predicate. Thus the predicate $P(a)$ defined by (18) is equivalent to the $P(a)$ defined by (22) and (23). Thus we have proved that the $P(a)$ of (18) is expressible in the form $(Ex)R(a,x)$ where R is general recursive.

As a matter of fact, by a result of Péter, this R is itself primitive recursive, if A, B and C are such; [12] but in any case, by the remark at the end of **6**, it follows without use of Péter's result that $P(a)$ is expressible in the form $(Ex)R(a,x)$ with an R which is primitive recursive.

We get another example, if instead of assuming that $A(a)$, $B(a,b)$ and $C(a,b,c)$ are general recursive, we assume merely that they are expressible in the respective forms $(Ex)S(a,x)$, $(Ex)T(a,b,x)$ and $(Ex)U(a,b,c,x)$ where S, T and U are general recursive. The reduction of $P(a)$ to the form

[12] [13]. The recursion equations for the representing function of R have the form of a double recursion, p. 493, with no nesting of ϕ's, and so by pp. 508-9 the function is primitive recursive.

$(Ex)R(a,x)$ where R is general recursive will go through with this alteration in the definition of $P(a)$, since again only existential quantifiers come to the front. This means that the form of the concept of formal provability is not altered by allowing a non-constructiveness in the rules of the formal system of the exact extent which occurs in the provability concept for a system with constructive rules.[13]

9. General aspects of the problem of reducing inductive definitions to explicit definitions. The two examples of **8** illustrate the treatment of inductive definitions with constructive direct clauses. In fact, when the notion of all predicates definable by successive inductive definitions with constructive direct clauses is made precise in a certain quite natural manner, then the method of these examples can be used to prove the general theorem that all such predicates are expressible in the form $(Ex)R(a_1,\cdots,a_n,x)$ where R is general recursive.[14]

Conversely, every predicate expressible in this form can be introduced by a series of inductive definitions with constructive direct clauses. Such a series is obtainable by the process of arithmetizing the metamathematical definitions for a suitable formal system which is consistent and complete for the proof of formulas expressing the true values of the predicate $(Ex)R(a_1,\cdots,a_n,x)$.

In the principal example of this paper, which follows, we accomplish the reduction of a certain particular inductive definition with non-constructive direct clauses.

However, our technique does not afford a general solution of the problem of reducing inductive definitions with non-constructive direct clauses to explicit ones, but is merely one which heuristically may lead to a reduction in particular cases. To begin with, the technique cannot always succeed in accomplishing reduction, since it is possible by inductive definition with non-constructive direct clauses to define a predicate which classically is non-elementary.[15] Moreover, the failure by the technique to accomplish the reduction of a given inductive definition would not in itself establish the non-elementary character of the predicate. No technique can exist which would afford a general solution of the problem in this sense.[16]

---

[13] For another treatment of this, see [10] § 14.

[14] This is contained in a manuscript of the author's which is not yet in form for publication.

[15] The definition of $M(a,k)$ in [10] § 17 can be written as an inductive definition.

[16] Using the predicate $T_1(z,x,y)$ from [10] § 4 or that from [7] § 2, we can introduce a parameter e into the inductive definition of $M(a,k)$ so that the resulting

The foregoing remarks on the non-constructive case are not precise, since we have not given an exact general description of inductive definition; but such a description can be given in a natural manner for the purpose of the present discussion. In particular, it would be required that the predicates presupposed in the statement of the clauses should be either elementary or defined by previous inductive definitions of the same type.

While the intuitionistic methods suffice for our example, it appears quite possible that the reduction technique might succeed for some examples classically but not intuitionistically. We know that the reduction of elementary predicates to the normal forms which was described in **6** is not always valid intuitionistically; and no reason is seen why there may not be inductively defined predicates reducible to the normal forms classically but not even elementary from the intuitionistic standpoint.[17]

10. Recursive definition of a function by a number. We shall give a minimum of preliminaries to the inductive definition of our principal example, confining ourselves chiefly to items relevant to the reduction.

We use, from the theory of general recursive functions,[18] a certain primitive recursive predicate $T_1(z, x, y)$ and a certain primitive recursive function $U(y)$. We shall write here simply "T" for "T_1."

Where $A(x, y)$ is any number-theoretic predicate, we use $\mu y A(x, y)$ to denote the least y such that $A(x, y)$ is true. Thus $\mu y A(x, y)$ is a function of the remaining variable x, defined for those natural numbers as values of x for which $(Ey)A(x, y)$ is true, and undefined for other values of x.

At this point we are liberalizing our use of the term function to allow *partial* number-theoretic functions which are not assumed to be defined for all arguments in the domain of natural numbers. The partial functions, as we use the term, include the ordinary or complete functions.

---

predicate $M_e(a, k)$ has the properties

$$[(x)(x \leq k \rightarrow \bar{T}_1(e, e, x))] \rightarrow M_e(a, k) \equiv M(a, k)$$

and

$$[(Ex)(x \leq k \,\&\, T_1(e, e, x))] \rightarrow M_e(a, k+1) \equiv M_e(a, k).$$

Then if $(Ex)T_1(e, e, x)$, the predicate $M_e(a, k)$ is elementary; while if $(x)\bar{T}_1(e, e, x)$, the predicate $M_e(a, k)$ is equivalent to $M(a, k)$ and hence classically non-elementary. By [10] § 5 or [7] § 2, the predicate $(Ex)T_1(a, a, x)$ is non-recursive. Hence by [1] § 7 or [10] § 12, there can be no general technique for determining whether a given number e has the property $(Ex)T_1(e, e, x)$. and therefore whether the predicate $M_e(a, k)$ is elementary.

[17] These remarks on the intuitionistic case are conjectures, which perhaps the theory being developed in [11] and [12] may provide the means for resolving.

[18] [10] §§ 4, 7.

In writing equality relationships between partial functions, we use the symbol $\simeq$ rather than $=$ to indicate the possibility of indefinition of the values. Thus $\phi(x) \simeq \psi(x)$, read, according to the context, either as referring to a particular x or as referring to any x, means that, for the x considered, if $\phi(x)$ and $\psi(x)$ are both defined, they have the same value, and if either is undefined, the other is. For example, with the symbol $\simeq$, the equality $\phi(x) \simeq \phi(x) + 1$ is not contradictory, if $\phi(x)$ is that partial function of x which is undefined for every value of x.

The preceding, and following, remarks are written out for functions of one variable, but apply analogously to functions of n variables, for any positive integer n.

An important partial function $\Phi_1(z, x)$ of two variables, which we shall here write omitting the subscript "1," is defined thus,

$$\Phi(z, x) \simeq U(\mu y T(z, x, y)). \tag{24}$$

Let $\phi(x)$ be a partial function of x. We say that the natural number e *defines ϕ recursively*, if

$$\phi(x) \simeq \Phi(e, x). \tag{25}$$

A notion of *partial recursive* function is obtained by extending the notion of general recursive definition to partial functions retaining the characteristic feature of the former as applied now to the set of the arguments for which a partial function is defined.

According to a fundamental theorem in the theory of general and partial recursive functions,[19] if $\phi(x)$ is general or partial recursive, then (25) holds for some natural number e.

Conversely, for any e, the function $\phi(x)$ defined by (25) is partial recursive, and therefore in the case that it is completely defined general recursive. This follows from the result that for any general recursive $A(x, y)$, the function $\mu y A(x, y)$ is partial recursive.[20]

Note that, if z is a fixed number, the condition that $\Phi(z, x)$ be defined for a given value of x as argument is as follows,

$$\{\Phi(z, x) \text{ is defined}\} \equiv (Ey)T(z, x, y). \tag{26}$$

The predicate $T(z, x, y)$ is so chosen, in the most recent version of the theory, that for a fixed z and x, $T(z, x, y)$ is true for at most one y. Hence,

$$T(z, x, y) \rightarrow \Phi(z, x) = U(y). \tag{27}$$

---

[19] [7] IV, [10] § 7.

[20] [7] V, [10] §§ 3, 6.

In stating this theory for functions of n variables, we start with a $T_n(z, x_1, \cdots, x_n, y)$ and define from it a $\Phi_n(z, x_1, \cdots, x_n)$.

There is a certain primitive recursive function $S_1^1(z, y)$ with the property that, if e defines recursively a partial function $\phi(a, x)$ of two variables a and x, then, for each fixed a, $S_1^1(e, a)$ defines recursively $\phi(a, x)$ considered as function of the one remaining variable x. Similarly there is a $S_n^m(z, y_1, \cdots, y_m)$ for any m parameters and n remaining variables.[21]

11. Ordinal representation. By n_O we shall denote the primitive recursive function defined thus: $0_O = 1$, $(n+1)_O = 2^{n_O}$.

Let n range over the natural numbers, and y_n be a number depending on n. By saying that a number y defines y_n recursively as function of n_O, we mean that there is a function $\phi(x)$ which takes as values $y_0, y_1, y_2, \cdots$ when x takes as values $0_O, 1_O, 2_O, \cdots$, respectively, and which is defined recursively by y. What that $\phi(x)$ may be for other values of x, i. e., whether or not defined and with what values if defined, is immaterial.

The class O and relation $<_O$ are now defined by the following simultaneous transfinite induction.

*O*1. $1 \in O$. *O*2. If $y \in O$, then $2^y \in O$ and $y <_O 2^y$. *O*3. If, for each n, $y_n \in O$ and $y_n <_O y_{n+1}$, and if y defines y_n recursively as function of n_O, then $3 \cdot 5^y \in O$ and, for each n, $y_n <_O 3 \cdot 5^y$. *O*4. If $x \in O$, $y \in O$, $z \in O$, $x <_O y$ and $y <_O z$, then $x <_O z$. *O*5. $a \in O$ and $a <_O b$ only as required by *O*1-*O*4.

Briefly, the rôle of the class O and relation $<_O$ in the theory of constructive ordinals is this.[22] The natural numbers which $\in O$ are mapped many-one on the ordinal numbers of a segment of the Cantor first and second number classes. The relation $<_O$ partially orders the former, and becomes the simple ordering relation of the latter under the mapping. The segment of ordinals on which the mapping takes place constitutes the so-called constructive first and second number classes.

The proof of our principal result we shall give in three main parts, which occupy the next three sections, and which will be assembled to give the theorem in **15**.

12. Analysis of O and $<_O$ in terms of $C(b)$ and Q. The transitivity clause *O*4 creates a difficulty for direct reduction of the definition of O. We shall get around this by introducing another relation $a \in C(b)$ to take the place of $a <_O b$. For each b which $\in O$, $C(b)$ will be the class of all numbers a such that $a <_O b$. With this $C(b)$ we shall define a Q equivalent to the O.

---

[21] [9] p. 153.

[22] [3], [2], [9].

The inductive definition of $C(b)$ is as follows.

$C1$. If $y \neq 0$, $C(2^y) = \{y\} + C(y)$. $C2$. $C(3 \cdot 5^y) = \sum_{n=0}^{\infty} [\{\Phi(y, n_O)\} + C(\Phi(y, n_O))]$, where terms of the sum for which $\Phi(y, n_O)$ is undefined contribute no elements to $C(3 \cdot 5^y)$. $C3$. $a \,\epsilon\, C(b)$ only as required by $C1$-$C2$.

When a predicate has been defined by induction, we may use proof by induction, in a form which corresponds to the form of the definition by induction, to establish properties of the predicate. This method is to be used in establishing the following lemmas. The proof of (VII) is given in detail for illustration.

Lemmas. (I) *If* $a \,\epsilon\, O$, *then* $a \neq 0$. (II) *If* $a <_O b$, *then* $b \neq 1$. (Use (I).) (III) $C(1)$ *is vacuous.* (IV) *If* $a <_O b$, *then* $a \,\epsilon\, O$ *and* $b \,\epsilon\, O$. (V) *If* $a <_O 2^y$, *then either* $a = y$ *or* $a <_O y$. (Use (IV).) (VI) *If* $a <_O 3 \cdot 5^y$, *then for some* n, *either* $a = y_n$ *or* $a <_O y_n$, *where* $y_n = \Phi(y, n_O)$. (Use (IV).)

(VII) *If* $b \,\epsilon\, O$, *then* $a \,\epsilon\, C(b) \rightarrow a <_O b$. Proof is by mathematical induction, in a form corresponding to the definition of O by induction, as follows. The parts of the proof numbered 1, 2, 3 correspond to the clauses $O1$, $O2$, $O3$, respectively, of the definition.

1. By (III), $a \,\epsilon\, C(1)$ cannot hold, and hence vacuously, $a \,\epsilon\, C(1) \rightarrow a <_O 1$.

2. Assume that $y \,\epsilon\, O$, and (as hypothesis of the induction) that $a \,\epsilon\, C(y) \rightarrow a <_O y$. By $O2$, then $2^y \,\epsilon\, O$ and $y <_O 2^y$. Assume (as hypothesis of the implication to be proved) that $a \,\epsilon\, C(2^y)$. By $C1$, either $a = y$ or $a \,\epsilon\, C(y)$. If $a = y$, then $a <_O 2^y$. If $a \,\epsilon\, C(y)$, then by the hypothesis of the induction, $a <_O y$, and hence $a <_O 2^y$ by (IV) and $O4$. Thus in both cases, $a <_O 2^y$. This was under the assumption $a \,\epsilon\, C(2^y)$. Therefore, $a \,\epsilon\, C(2^y) \rightarrow a <_O 2^y$.

3. Assume that, for every n, $y_n \,\epsilon\, O$ and $y_n <_O y_{n+1}$, that y defines y_n recursively as function of n_O, and (as hypothesis of the induction) that, for every n, $a \,\epsilon\, C(y_n) \rightarrow a <_O y_n$. By $O3$, $3 \cdot 5^y \,\epsilon\, O$ and, for every n, $y_n <_O 3 \cdot 5^y$. Assume (as hypothesis of the implication to be proved) that $a \,\epsilon\, C(3 \cdot 5^y)$. By $C2$, for some n, either $a = \Phi(y, n_O)$ or $a \,\epsilon\, C(\Phi(y, n_O))$. Since $y_n = \Phi(y, n_O)$, we have either $a = y_n$ or $a \,\epsilon\, C(y_n)$. If $a = y_n$, then $a <_O 3 \cdot 5^y$. If $a \,\epsilon\, C(y_n)$, then by the hypothesis of the induction, $a <_O y_n$, and by (IV) and $O4$, $a <_O 3 \cdot 5^y$. Thus in both cases, $a <_O 3 \cdot 5^y$. Therefore, $a \,\epsilon\, C(3 \cdot 5^y) \rightarrow a <_O 3 \cdot 5^y$.

The proof by induction is now completed.

(VIII) *If* $b \,\epsilon\, O$, *then* $a <_O b \rightarrow a \,\epsilon\, C(b)$. Proof is similar, using (I), (II), (IV), (V) and (VI).

The inductive definition of Q is as follows.

$Q1$. $1 \in Q$. $Q2$. If $y \in Q$, then $2^y \in Q$. $Q3$. If, for each n, $y_n \in Q$ and $y_n \in C(y_{n+1})$, and if y defines y_n recursively as a function of n_O, then $3 \cdot 5^y \in Q$. $Q4$. $a \in Q$ only as required by $Q1$-$Q3$.

We can now establish, using (IV), (VII) and (VIII),

$$a \in O \equiv a \in Q, \tag{28}$$

$$a <_O b \equiv b \in Q \;\&\; a \in C(b). \tag{29}$$

13. Reduction of $a \in C(b)$. Rewriting the inductive definition of $C(b)$ in symbols as an equivalence,

$$\begin{aligned}(30)\quad a \in C(b) \equiv\ & (Ey)\{y \neq 0 \;\&\; b = 2^y \;\&\; (a = y \vee a \in C(y))\}\\ & \vee (Ey)\{a = 3 \cdot 5^y \;\&\; (En)[(\Phi(y, n_O) \text{ is defined}) \;\&\; (a = \Phi(y, n_O)\\ & \vee a \in C(\Phi(y, n_O)))]\}.\end{aligned}$$

Thence, using (26) and (27),

$$\begin{aligned}(31)\quad a \in C(b) \equiv\ & (Ey)\{y \neq 0 \;\&\; b = 2^y \;\&\; (a = y \vee a \in C(y))\}\\ & \vee (Ey)\{a = 3 \cdot 5^y \;\&\; (En)(Ez)[T(y, n_O, z) \;\&\; (a = U(z)\\ & \vee a \in C(U(z)))]\}.\end{aligned}$$

Substituting "$(Ex)V(a, b, x)$" for "$a \in C(b)$," all the existential quantifiers on the right come to the front, and so by the method of **8** we determine a general recursive (and in fact, primitive recursive) predicate $V(a, b, x)$ such that

$$a \in C(b) \equiv (Ex)V(a, b, x). \tag{32}$$

14. Reduction of $a \in Q$. If the natural number a is of the form 2^y, then $y = (a)_1$; if of the form $3 \cdot 5^y$, then $y = (a)_3$. Rewriting the definition of Q, with the use of these expressions for y,

$$\begin{aligned}(33)\quad a \in Q \equiv a = 1 \vee \{a = 2^{(a)_1} \;\&\; (a)_1 \in Q\} \vee \{& a = 3 \cdot 5^{(a)_3}\\ & \& \; (n)[\Phi((a)_3, n_O) \text{ is defined}]\\ & \& \; (n)[\Phi((a)_3, n_O) \in Q]\\ & \& \; (n)[\Phi((a)_3, n_O) \in C(\Phi((a)_3, (n+1)_O))]\}.\end{aligned}$$

Using (26), (27) and (32),

$$\begin{aligned}(34)\quad a \in Q \equiv a = 1 \vee \{a = 2^{(a)_1} \;\&\; (a)_1 \in Q\} \vee \{& a = 3 \cdot 5^{(a)_3}\\ & \& \; (n)(Ey)T((a)_3, n_O, y)\\ & \& \; (n)(y)[T((a)_3, n_O, y) \rightarrow U(y) \in Q]\\ & \& \; (n)(y)(z)[(T((a)_3, n_O, y) \;\&\; T((a)_3, (n+1)_O, z))\\ & \qquad \rightarrow (Ex)V(U(y), U(z), x)]\}.\end{aligned}$$

Substituting "$(x)(Ey)R(a,x,y)$" for "$a \epsilon Q$," with suitable changes in the bound variables,

$$
\begin{aligned}
(35) \quad (x)(Ey)R(a,x,y) \equiv a = 1 \vee \{a = 2^{(a)_1} \,\&\, (x_1)(Ey_1)R((a)_1, x_1, y_1)\} \\
\vee \{e = 3 \cdot 5^{(a)_3} \\
\&\, (x_2)(Ey_1)T((a)_3, (x_2)_O, y_1) \\
\&\, (x_2)(x_3)[T((a)_3, (x_2)_O, x_3) \rightarrow (x_4)(Ey_2)R(U(x_3), x_4, y_2)] \\
\&\, (x_2)(x_3)(x_4)[(T((a)_3, (x_2)_O, x_3) \,\&\, T((a)_3, (x_2+1)_O, x_4)) \\
\rightarrow (Ey_3)V(U(x_3), U(x_4), y_3)]\}.
\end{aligned}
$$

The determination of $R(a,x,y)$ as a general recursive (and in fact, primitive recursive) predicate such that

$$(36) \qquad a \epsilon Q \equiv (x)(Ey)R(a,x,y)$$

can now be accomplished by the technique of **8**; in so doing, the following particulars may be noted.

The distribution of subscripts on the bound variables in (35) is such that, when the advancement of quantifiers on the right is carried through in a suitable way, they will come to the front in the order

$$(x_1)(x_2)(x_3)(x_4)(Ey_1)(Ey_2)(Ey_3).$$

To see that this can be done intuitionistically, note the following. The first members of the two implications are recursive, so the special condition for the intuitionistic use of (10*) and (11*) is fulfilled. In the advancement of universal quantifiers across the second disjunction, (12*) will have to be used. If (x_1) is brought first to the front of the middle disjunctive member, the special conditions for the application of (12*) to advance it across the disjunction are realized, since $a = 3 \cdot 5^{(a)_3}$ is recursive and excludes the part $a = 2^{(a)_1}$, and hence the whole, of the operand of (x_1). If next (x_2), (x_3) and (x_4) are brought one at a time to the front of the last disjunctive member, the special conditions for the advancement of each across the disjunction are realized, since $a = 2^{(a)_1}$ is recursive and excludes the part $a = 3 \cdot 5^{(a)_3}$, and hence the whole, of the operand of the quantifier. For the advancement of the universal quantifiers across the first disjunction, (7*) suffices, since $a = 1$ is recursive.

In the subsequent contraction, we can use (16) and (17), or one of these and the other of (14) and (15).

15. The form of the predicates $a \epsilon O$ and $a <_O b$. By (28) and (36),

$$(37) \qquad a \epsilon O \equiv (x)(Ey)R(a,x,y).$$

By (29), (32) and (36),

$$(38) \qquad a <_O b \equiv (x)(Ey)R(b, x, y) \;\&\; (Ex)V(a, b, x).$$

Advancing the quantifiers and contracting, if we set $S(a, b, x, y) \equiv R(b, x, (y)_1)$ $\&\; V(a, b, (y)_2)$, then

$$(39) \qquad a <_O b \equiv (x)(Ey)S(a, b, x, y)$$

where $S(a, b, x, y)$ is primitive recursive. Thus we establish —

THEOREM 1. *The predicates* $a \epsilon O$ *and* $a <_O b$ *are expressible in the respective forms* $(x)(Ey)R(a, x, y)$ *and* $(x)(Ey)S(a, b, x, y)$ *where* R *and* S *are primitive recursive.*

The crux of the foregoing reduction is to make all the universal quantifiers in the right member of (35) come to the front ahead of the existential. In general, the problem in applying the reduction technique is to make the quantifiers come to the front in such an order that after contraction they will be the same sequence of quantifiers as in the form substituted for the predicate, for some choice of that form. An attempt to reduce the predicate $a \epsilon O$ of the system S_1 of notation for ordinals,[23] which belongs to an earlier version of the Church-Kleene theory, failed on this point.

16. Recursive mappings of the classes $\hat{a}(a \epsilon O)$ and $\hat{a}(x)(Ey)T(a, x, y)$, each on a part of the other. Using the $R(a, x, y)$ of the preceding theorem, we introduce the partial function $\phi(a, x) \simeq \mu y R(a, x, y)$. This is partial recursive, by the result on the μ-operator cited in **10**. Then, for each fixed a, we introduce $\phi_a(x) \simeq \phi(a, x)$ considered as function of the remaining variable x. We let e be a number defining $\phi(a, x)$ recursively, and set $F(a) = S_1^1(e, a)$. Then $F(a)$ is primitive recursive, and for each fixed a, $F(a)$ defines $\phi_a(x)$ recursively. For the fixed a, the partial recursive function $\phi_a(x)$ is completely defined, and therefore general recursive, if and only if $(x)(Ey)R(a, x, y)$. Also, by (25) and (26), the condition that $F(a)$ define a general recursive function is $(x)(Ey)T(F(a), x, y)$. Therefore,

$$(40) \qquad (x)(Ey)R(a, x, y) \equiv (x)(Ey)T(F(a), x, y).$$

Restating this with the use of (37),

$$(41) \qquad a \epsilon O \equiv (x)(Ey)T(F(a), x, y).$$

By the construction of $F(a)$ which actually underlies this discussion,

$$(42) \qquad a = b \equiv F(a) = F(b).$$

---

[23] [9] p. 153.

We now have the first part of the next theorem.

To establish the inverse relationship, let $\psi(a,x) \simeq (\Phi(a,0) + \Phi(a,1) + \cdots + \Phi(a,x) + x)_O$. This function is partial recursive. For a fixed a, we introduce $\psi_a(x) \simeq \psi(a,x)$ considered as function of x only. Let f be a number defining $\psi(a,x)$ recursively, and set $G(a) = 3 \cdot 5^{S_1^1(f,a)}$.

For any given a, let $\phi(x)$ be the partial function defined recursively by the number a. If this function is general recursive, then the values of $\psi_a(x)$ for $x = 0_O, 1_O, 2_O, \cdots$ are $(y_0)_O, (y_1)_O, (y_2)_O, \cdots$, respectively, where $y_0, y_1, y_2, \cdots$ are successively increasing natural numbers; and so by $O3$, $G(a) \epsilon O$. In fact, $G(a)$ then represents the ordinal ω. Conversely, if $G(a) \epsilon O$, then by the definition of O, the values of $\psi_a(x)$ for $x = 0_O, 1_O, 2_O, \cdots$ must all be defined, which can only be the case if $\phi(x)$ is completely defined. Therefore, using (25) and (26),

$$(43) \qquad (x)(Ey)T(a,x,y) \equiv G(a) \epsilon O.$$

By the construction of $G(a)$,

$$(44) \qquad a = b \equiv G(a) = G(b).$$

THEOREM 2. *The set O of the numbers which represent constructive ordinals is mapped one-to-one by a primitive recursive function $F(a)$ on a subset of the set of the numbers which define general recursive functions recursively; and inversely, the latter set is mapped one-to-one by a primitive recursive function $G(a)$ on a subset of the former.*

This is suggestive of the Cantor continuum hypothesis,[24] but the analogy is deficient, since under the inverse mapping all the images represent the single ordinal ω.

In the proof of (40), the only property of $R(a,x,y)$ which we used was its general recursiveness. Therefore by the same method we can set up a primitive recursive function $H(a)$ such that

$$(45) \qquad (x)(Ey)T_2(a,a,x,y) \equiv (x)(Ey)T(H(a),x,y).$$

17. Specific character of the reduction given for $a \epsilon O$ and $a <_O b$. It is known that the predicate $(x)(Ey)T_2(a,a,x,y)$ is not expressible in the form $(Ex)(y)M(a,x,y)$ where M is general recursive, and *a fortiori* not in any of the normal forms of **6** with fewer quantifiers.[25] From this fact, we

[24] A constructive analog of the continuum hypothesis which is false is given in [15] § 10.

[25] [10] § 5.

shall infer the like successively for $(x)(Ey)T(a,x,y)$, $a \epsilon O$, and, with b as additional variable, $a <_O b$.

Suppose we did have

$$\text{(a)} \qquad (x)(Ey)T(a,x,y) \equiv (Ex)(y)N(a,x,y)$$

with a recursive N. Then by (45) we should have

$$\text{(b)} \qquad (x)(Ey)T_2(a,a,x,y) \equiv (Ex)(y)N(H(a),x,y).$$

Since then $N(H(a),x,y)$ would be a recursive $M(a,x,y)$, this is impossible. Hence (a) is impossible.[26]

Then likewise, if we had

$$\text{(c)} \qquad a \epsilon O \equiv (Ex)(y)P(a,x,y)$$

with a recursive P, using (43), $P(G(a),x,y)$ would be a recursive $N(a,x,y)$; and so (c) is impossible.

Finally, suppose that we had

$$\text{(d)} \qquad a <_O b \equiv (Ex)(y)Q(a,b,x,y)$$

with a recursive Q. Then we should have by substitution,

$$\text{(e)} \qquad a <_O 2^a \equiv (Ex)(y)Q(a,2^a,x,y).$$

By $O2$ and (IV),

$$\text{(46)} \qquad a <_O 2^a \equiv a \epsilon O.$$

From (e), we should have by (46),

$$\text{(f)} \qquad a \epsilon O \equiv (Ex)(y)Q(a,2^a,x,y).$$

Since then $Q(a,2^a,x,y)$ would be a recursive $P(a,x,y)$, this is impossible. Hence (d) is impossible.

THEOREM 3. *The predicates $a \epsilon O$ and $a <_O b$ are not expressible in the forms dual to those of Theorem 1, nor in any of the forms with fewer quantifiers.*

AMHERST COLLEGE,
AMHERST, MASS.

---

[26] This supplies the proof of [7] XI from [10] § 5 referred to in [10] § 4 footnote (9)

BIBLIOGRAPHY.

CHURCH, ALONZO. [1] "An unsolvable problem of elementary number theory," *American Journal of Mathematics*, vol. 58 (1936), pp. 345-363. [2] "The constructive second number class," *Bulletin of the American Mathematical Society*, vol. 44 (1938), pp. 224-232.

CHURCH, ALONZO and KLEENE, S. C. [3] "Formal definitions in the theory of ordinal numbers," *Fundamenta Mathematicae*, vol. 28 (1936), pp. 11-21.

GÖDEL, KURT. [4] "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I," *Monatshefte für Mathematik und Physik*, vol. 38 (1931), pp. 173-198. [5] "On undecidable propositions of formal mathematical systems," mimeographed notes on lectures at the Institute for Advanced Study (1934).

HILBERT, DAVID and BERNAYS, PAUL. [6] *Grundlagen der Mathematik*, vol. 1 (1934), Berlin (Springer).

KLEENE, S. C. [7] "General recursive functions of natural numbers," *Mathematische Annalen*, vol. 112 (1936), pp. 727-742. [8] "A note on recursive functions," *Bulletin of the American Mathematical Society*, vol. 42 (1936), pp. 544-546. [9] "On notation for ordinal numbers," *Journal of Symbolic Logic*, vol. 3 (1938), pp. 150-155. [10] "Recursive predicates and quantifiers," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 41-73. [11] "On the interpretation of intuitionistic number theory," *Bulletin of the American Mathematical Society*, vol. 48 (1942), abstract 85, p. 51.

NELSON, DAVID. [12] "Recursive functions and intuitionistic number theory," under preparation.

PÉTER, ROZSA. [13] "Über die mehrfache Rekursion," *Mathematische Annalen*, vol. 113 (1936), pp. 489-527.

TURING, A. M. [14] "On computable numbers, with an application to the Entscheidungsproblem," *Proceedings of the London Mathematical Society*, ser. 2, vol. 42 (1937), pp. 230-265. [15] "Systems of logic based on ordinals," *ibid.*, vol. 45 (1939), pp. 161-228.

THE RESULTANT OF A LINEAR SET.*

By Ernst Snapper.

Introduction. Hentzelt and Noether [1] have discussed the resultant of an ideal consisting of polynomials in n variables. In the present paper the corresponding theory for a linear subset of an m-dimensional vector space whose scalar domain consists of polynomials in n variables is developed. The results of [1] are shown to hold equally well for any number of dimensions, a step toward a theory of matrices whose elements are such polynomials.

Assuming that the linear sets have been transformed by means of a linear transformation (see **2**), the main results are: *With every linear set L of such a vector space, a resultant ρ is associated which is a polynomial in n variables. This resultant vanishes for, and only for, the common roots of the polynomials of the ideal $L/Cl(L)$.* (See **6.**) *Furthermore, if $L_2 \subseteq L_1$, then $L_2 = L_1$ if and only if L_1 and L_2 have the same rank and resultant.*

This demonstrates the importance of the algebraic manifold of the ideal $L/Cl(L)$ for the linear set L. The resultant ρ can be factored into exactly n factors $\rho = \prod_{i=1}^{n} \rho^{(i)}$ such that every common root of the polynomials of $L/Cl(L)$ corresponds to one of these factors. Furthermore, the multiplicities of the irreducible factors of $\rho^{(i)}$ (the multiplicity being the product of degree and exponent) are equal to the number of independent restclasses of certain factor groups which are uniquely determined by L. The last statement of the results gives a criterion for the existence of a polynomial solution of a system of linear equations with polynomial coefficients. (See Theorem 5.3.) This is the analogue of the theorem (see [2]) that in an algebraic number system, a system of linear equations can be solved simultaneously if and only if the matrix of the system and the "augmented" matrix have the same rank and the same highest dimensional determinantal factor.

Since the methods of Hentzelt and Noether [1] are immediately applicable to vector spaces, direct reference is made to their proofs and additional details are given only where necessary.

Notation. Scalars are indicated by lower case Greek letters; linear sets, matrices and integral domains by capital Latin letters; vectors by lower case Latin letters and ideals by lower case German letters.

* Received October 21, 1942.

1. The linear subset of a general vector space. Let V_m be an m-dimensional vector space, consisting of row vectors with m components where the components form an integral domain S, called the scalar domain of the vector space. A linear subset L of V_m is a subset closed under vector subtraction and scalar multiplication. The quotient L_1/L_2 of two linear sets, the quotient $L/\mathfrak{a}$ of a linear set by an ideal, the product $\mathfrak{a}L$ of an ideal and a linear set, the closure $Cl(L)$ of a linear set and the notion of a closed set have been previously defined in [3]. We also use these definitions for denumerably infinite dimensional vector spaces, whose vectors have a denumerably infinite number of components of which only a finite number are different from zero. Returning to a finite number of dimensions m, the i-th determinantal factor $\mathfrak{d}_i$ of a linear set L (or of a matrix A with m columns) is the ideal generated by the minors of dimension $m - i$ of the matrices whose rows are vectors of L (or just by the minors of dimension $m - i$ of A) for $i = 0, \cdots, m - 1$. For $i \geqq m$ we define $\mathfrak{d}_i = S$ as is done by Fitting [4]. The j-th invariant factor of L is, for $j = 1, 2, \cdots$, defined as $\mathfrak{e}_j = \mathfrak{d}_{k+j-1}/\mathfrak{d}_{k+j}$, where $\mathfrak{d}_k$ is the first non-zero determinantal factor of L. Hence, a linear set or a matrix has an infinite number of determinantal factors and invariant factors, and $\mathfrak{d}_{i-1} \subseteq \mathfrak{d}_i$. Furthermore, if the rows of the matrix A form a set of generators of L, the i-th determinantal and hence invariant factors of L are equal to those of A.

Let us now assume that every ideal of the scalar domain S has a finite ideal basis. The rank r of a linear set L is then defined as the maximal number of vectors of L which are linearly independent with respect to S. It can easily be proved [1, pp. 56-58] that L and $Cl(L)$ always have the same rank and that $Cl(L)$ is the only closed linear set (called "Grundmodul" in [1]) which contains L and has the same rank as L. Hence, a linear set is closed if and only if it is not contained in a different linear set which has the same rank. Finally, $Cl(L) = L/\mathfrak{d}_{m-r}$ [1, Theorem III, p. 58].

The factor group $Cl(L) \div L$ is a module with a finite number of generators and with S as operator domain. With each set of generators of such a "finite" module, a null space is associated which is the linear set consisting of the vectors which annul the generator set. In [4, p. 197], the determinantal factors of such a null space are proved to be independent of the underlying generator set and are consequently called the determinantal factors of the module. For the same reason, the invariant factors of these null spaces will be called the invariant factors of the module. The first non-zero determinantal factor of a module will be called the norm of the module. It is clear that if $Cl(L)$ has a linearly independent basis which is transformed by the matrix A into a set of generators of L, the determinantal factors and invariant factors

of A and of $Cl(L) \div L$ are the same and, consequently, the norm of $Cl(L) \div L$ is equal to the first non-zero determinantal factor of A. If S is a principal ideal ring, any generator of the norm of $Cl(L) \div L$ will be considered as a norm and will be denoted by $\nu(Cl(L) \div L)$.

Finally, if S is a Euclidean domain and L has rank r, $\mathfrak{e}_1 \subseteq \mathfrak{e}_2 \subseteq \cdots$ and the generators δ_i and ϵ_i of the ideals $\mathfrak{d}_i$ and $\mathfrak{e}_i$ respectively can be chosen such that $\delta_{m-j} = \prod_{i=r-j+1}^{r} \epsilon_i$ for $j = 1, \cdots, r$. Since we can then choose (see [1, pp. 55, 56 and 60]) a linearly independent basis $u_1, \cdots, u_r$ for $Cl(L)$ such that $\epsilon_1 u_1, \cdots, \epsilon_r u_r$ is a basis for L, the norm of $Cl(L) \div L$ is the scalar δ_{m-r} and the non-zero determinantal factors and invariant factors of L are equal to those of $Cl(L) \div L$. If S consists of polynomials in one variable with coefficients in a field P, the degree of δ_{m-r} is equal to the number of restclasses of $Cl(L) \div L$ which are linearly independent with respect to P. Furthermore, bearing in mind that in the present notation the highest dimensional invariant factor of L is called $\mathfrak{e}_1$, the following theorems of [1] are used: I [p. 57], IV and V [p. 60].

2. Linear transformation of variables. Let $\bar{V}_m$ be an m-dimensional vector space which consists of row vectors with m components and whose scalar domain $\bar{S} = P[\eta_1 \cdots \eta_n]$ consists of polynomials in n variables $\eta_1, \cdots, \eta_n$ with coefficients in a field P. If we adjoin the variables $\gamma_{2,1}, \cdots, \gamma_{n,n-1}$ to P (see [1, Section 3]), the scalar domain becomes $\bar{S}(\gamma) = P(\gamma)[\eta_1, \cdots, \eta_n]$. Furthermore every linear set $\bar{L}$ of $\bar{V}_m$ has then to be extended to the linear set $\bar{L}(\gamma)$ consisting of the vectors $\bar{v}(\gamma) = \sum_j \omega_j(\gamma)\bar{v}_j$, where $\omega_j(\gamma)$ denotes an arbitrary monomial of the variables $\gamma_{i,j}$ and where the vector $\bar{v}_j$ is a vector of $\bar{L}$ (disregarding multiplication by elements of $P(\gamma)$ as is done in [1, p. 62, equations 13]). If we then transform the variables $\eta_1, \cdots, \eta_n$ by the fixed, linear, reversible transformation $\eta = U(\xi)$, that is $\eta_1 = \xi_1$, $\eta_n = \gamma_{n,1}\xi_1 + \cdots + \gamma_{n,n-1}\xi_{n-1} + \xi_n$ (see [1, p. 61]), every linear set $\bar{L}(\gamma)$ is transformed into a linear subset L of the m-dimensional vector space V_m whose scalar domain $S = P(\gamma)[\xi_1, \cdots, \xi_n]$ consists of polynomials in n variables $\xi_1, \cdots, \xi_n$ with coefficients in $P(\gamma)$. We shall call a linear set L of V_m a transformed linear set if L can be obtained from a linear set $\bar{L}$ of $\bar{V}_m$ by first adjoining the variables γ_{ij} to P and then transforming the $\eta_1, \cdots, \eta_n$ by means of $\eta = U(\xi)$. The criterion, expressed in [1, p. 62, equations 15], holds without change, i. e. the linear set L is transformed if and only if in the expression $v = U(U^{-1}(v)) = U(\sum_j \omega_j(\gamma)\bar{v}_j) = \sum_j \omega_j(\gamma)U(\bar{v}_j)$, where v is an arbitrary vector of L, the vectors $U(\bar{v}_j)$ are again vectors of L.

We know from [1, Section 3] that these two processes of adjunction and linear transformation replace the ideals of $\bar{S}$ by the transformed ideals of S, which have the property of containing at least one polynomial which is regular with respect to ξ_1. The following theorem is the main reason why the methods of [1] are applicable to an arbitrary number of dimensions:

THEOREM 2. 1. *If the linear set L is the transform of the linear set $\bar{L}$, the i-th determinantal factor $\mathfrak{d}_i$ of L is the transform of the i-th determinantal factor $\bar{\mathfrak{d}}_i$ of $\bar{L}$ and the same holds for the invariant factors.*

Proof. The i-th determinantal factor $\mathfrak{d}_i$ of L is generated by the $(m-i)$-dimensional minors Δ of the matrices whose rows $v_1, \cdots, v_m$ are vectors of L. Since $U^{-1}(v_k) = \sum_j \omega_j(\gamma)\bar{v}_j$, where $\bar{v}_j \equiv 0(\bar{L})$, $U^{-1}(\Delta) = \sum_j \omega'_j(\gamma)\bar{\Delta}_j$, where $\bar{\Delta}_j$ is an element of $\bar{\mathfrak{d}}_i$. Consequently, $\mathfrak{d}_i$ is contained in the transform of $\bar{\mathfrak{d}}_i$. However, every matrix whose rows are vectors of $\bar{L}$ is transformed by $\eta = U(\xi)$ into a matrix whose rows are vectors of L, and hence every element of the ideal $\bar{\mathfrak{d}}_i$ is transformed into an element of the ideal $\mathfrak{d}_i$ which proves that the transform of $\bar{\mathfrak{d}}_i$ is equal to $\mathfrak{d}_i$. The statement about the invariant factors then follows immediately from [1, p. 77, Section 7] where it is proved that the quotient of two transformed ideals is equal to the transform of the quotient of these ideals.

As the transform of an ideal is the zero-ideal if and only if the ideal itself is the zero-ideal, we have as a corollary of Theorem 2. 1 that a linear set and its transform have the same rank.

3. The n closures of a linear set. Let V_m again be the m-dimensional vector space with scalar domain $S = P(\gamma)[\xi_1, \cdots, \xi_n]$. We shall now consider the denumerably infinite dimensional vector space $V^{(i-1)}$ with scalar domain $S^{(i)} = P(\gamma)[\xi_i, \cdots, \xi_n]$ for $i = 1, \cdots, n$. The fundamental vectors of $V^{(i-1)}$ are the vectors $\prod_{s=1}^{i-1} \xi_s^{k_s} f_j$, where $\prod_{s=1}^{i-1} \xi_s^{k_s}$ is any monomial of the variables $\xi_1, \cdots, \xi_{i-1}$ (each k_s can assume all positive integral values, zero included) and where f_j is an arbitrary fundamental vector of V_m for $j = 1, \cdots, m$. The scalar domain $S^{(i)}$, whose scalars will be indicated by the upper index i, consists of polynomials in $\xi_i, \cdots, \xi_n$ with coefficients in $P(\gamma)$, while the vectors of $V^{(i-1)}$ are linear combinations, with coefficients in $S^{(i)}$, of the fundamental vectors where only a finite number of the coefficients is different from zero.

Each vector v of V_m is associated with a unique vector of $V^{(i-1)}$, which we obtain by ordering the components of v with respect to the monomials of

the variables $\xi_1, \cdots, \xi_{i-1}$. (See [1, p. 64].) This correspondence is clearly an operator isomorphism T_{i-1} with respect to $S^{(i)}$ as operator domain, which associates a linear set $T_{i-1}(L) = L_{i-1}$ of $V^{(i-1)}$ with every linear set L of V_m. To the closure $Cl(L_{i-1})$ of L_{i-1}, there corresponds a linear subset of V_m which is called the $(i-1)$-th closure of L according to the following definition (see [1, definition V]):

DEFINITION 3.1. *The $(i-1)$-th closure $Cl_{i-1}(L)$ of a linear subset L of V_m consists of the vectors v of V_m for which we can find a non-zero scalar $\alpha^{(i)}$ of $S^{(i)}$ such that $\alpha^{(i)}v \equiv 0(L)$.*

Consequently, we always have the relationships $T_{i-1}(Cl_{i-1}(L)) = Cl(L_{i-1})$ and $Cl_i(L) \subseteq Cl_{i-1}(L)$. Furthermore, $Cl_0(L) = Cl(L)$.

THEOREM 3.1. *The closures of a transformed linear set are themselves transformed linear sets.*

The proof of this theorem is the same as that of [1, Theorem VI] if the following extension of the theorem of Dedekind and Mertens to vectors is used (see [1, p. 63]):

THEOREM OF DEDEKIND AND MERTENS. *Let $\alpha_{i_1 \ldots i_s}$ be variables and let $b_{j_1 \ldots j_s}$ be vectors whose t components are variables and let the vectors $c_{k_1 \ldots k_s}$ be defined by the product of the scalar polynomial and the vector polynomial*

$$\sum \alpha_{i_1 \ldots i_s} \zeta_1^{i_1} \cdots \zeta_s^{i_s} \cdot \sum b_{j_1 \ldots j_s} \zeta_1^{j_1} \cdots \zeta_s^{j_s} = \sum c_{k_1 \ldots k_s} \zeta_1^{k_1} \cdots \zeta_s^{k_s},$$

where the polynomials are of finite degree. Then, there exists an integer q such that $\mathfrak{a}^q B = \mathfrak{a}^{q-1} C$, where $\mathfrak{a}$, B and C are the modules which consist of the linear, rational integral combinations of the α's, b's and c's respectively and where $\mathfrak{a}^j$ consists of the linear, rational integral combinations of the monomials of degree j of the α's.

The reasoning of Dedekind's proof in [5], applied to each component of the b's and the c's, proves this extension immediately.

4. The factor module $Cl(L_{i-1}) \div L_{i-1}$. Let L be a transformed linear set of the same vector space V_m. Since $S^{(i)}$ is the scalar domain of the vector space $V^{(i-1)}$, the factor module $Cl(L_{i-1}) \div L_{i-1}$ has $S^{(i)}$ as operator domain. The following theorem shows that, although $V^{(i-1)}$ is an infinite dimensional vector space, the factor module $Cl(L_{i-1}) \div L_{i-1}$ has a finite number of generators (see [1, Theorem VII]):

THEOREM 4.1. *The factor module $Cl(L_{i-1}) \div L_{i-1}$ is operator isomorphic to the finite factor module $Cl(L'_{i-1}) \div L'_{i-1}$ with respect to $S^{(i)}$ as operator domain, where L'_{i-1} and its closure $Cl(L'_{i-1})$ are linear subsets of a finite dimensional vector space $V'^{(i-1)}$ with $S^{(i)}$ as scalar domain. Hence, $Cl(L_{i-1}) \div L_{i-1}$ is a finite module whose determinantal factors and invariant factors are equal to those of $Cl(L'_{i-1}) \div L'_{i-1}$. Clearly, these statements are still valid if the variables $\xi_{i+1}, \cdots, \xi_n$ are adjoined to $P(\gamma)$ and $S^{(i)}$ is replaced by $S'^{(i)} = P(\gamma, \xi_{i+1}, \cdots, \xi_n)[\xi_i]$.*

Proof. The theorem is proved by induction. (See [1, pp. 64-70]). For $i = 1$ the theorem is trivial since $V^{(0)}$ is equal to V_m and $S^{(1)}$ is equal to S. For $i = 2$ we observe that, as L is a transformed linear set, its highest dimensional non-zero determinantal factor is a transformed ideal (see Theorem 2.1) and consequently contains at least one polynomial which is regular with respect to ξ_1. From here on, the proof is exactly the same as that of [1, pp. 68-69], assuming that $i = 2$. Hence, for i the following induction hypotheses may be made: There exists an operator isomorphism F_{i-1} with respect to $S^{(i)}$ as operator domain which associates $Cl_{i-1}(L)$ with a linear subset of the denumerably infinite vector space $W^{(i-1)}$ whose scalar domain is $S^{(i)}$. The first s fundamental vectors of $W^{(i-1)}$ are denoted by $u_1, \cdots, u_s$ and the remaining ones by $k_0, k_1, \cdots$ *ad infinitum*, i. e. $W^{(i-1)} = u_1, \cdots, u_s, k_0, k_1, \cdots$ *ad infinitum*. Furthermore, $F_{i-1}(Cl_{i-1}(L)) = (Cl(L'_{i-1}), K_{i-1})$ and $F_{i-1}(L) = (L'_{i-1}, K_{i-1})$, where L'_{i-1} is a linear subset of the space $V'^{(i-1)}$ generated by the u's, and where K_{i-1} denotes the space generated by the k's. Finally, if instead of the linear transformation $\eta = U(\xi)$, we use the special linear transformation $\eta = U'_{i-1}(\xi, \zeta)$, that is

$$\eta_1 = \xi_1; \cdots; \eta_{i-1} = \gamma_{i-1,1}\xi_1 + \cdots + \xi_{i-1};$$
$$\eta_i = \gamma_{i,1}\xi_1 + \cdots + \gamma_{i,i-1}\xi_{i-1} + \zeta_i; \cdots; \eta_n = \gamma_{n,1}\xi_1 + \cdots + \gamma_{n,i-1}\xi_{i-1} + \zeta_n,$$

the above hypotheses still hold, and the linear sets and decompositions which then occur are transformed into the old ones by the linear transformation $U'^{-1}_{i-1} \cdot U$. The theorem can then be proved immediately for i. (See [1, p. 67].) In order to prove the theorem for $i + 1$, we first observe that the highest dimensional non-zero determinantal factor of L'_{i-1} contains at least one polynomial $\pi^{(i)}$ which is regular with respect to ξ_i. This follows from the fact that L'_{i-1} is the transform with respect to $U'^{-1}_{i-1} \cdot U$ of the corresponding linear set which occurs if we use U'_{i-1} instead of U as the linear transformation. Theorem 2.1 then asserts that the determinantal factors of L'_{i-1} are transformed ideals with respect to $U'_{i-1} \cdot U$. The rest of the proof can be copied from [1, pp. 68 and 69].

If the field P is infinite, the variables $\gamma_{i,j}$ of the transformation $\eta = U(\xi)$ can be specialized as elements of P in such a way that the n polynomials $\pi^{(i)}$ $(i = 1, \cdots, n)$ remain regular with respect to ξ_i. Consequently, Theorem 4.1 remains valid for such a specialization and the linear transformation $\eta = U(\xi)$, which was used to transform the linear sets into transformed linear sets, may then be considered as a transformation with coefficients in P.

5. Resultant and elementary divisor of a linear set. Let L again be a transformed linear set and let the variables $\xi_{i+1}, \cdots, \xi_n$ be adjoined to $P(\gamma)$. The scalar domain of $V^{(i-1)}$ and $V'^{(i-1)}$ is then the Euclidean domain $S'^{(i)}$ and the linear set L'_{i-1} has the properties described at the end of **1**. As the polynomial $\pi^{(i)}$ of the previous section is a polynomial of the highest dimensional non-zero determinantal factor $\mathfrak{d}_{s-r}$ of L'_{i-1}, the generators δ_j and ϵ_j of the determinantal factors and invariant factors respectively of L'_{i-1} can be considered as polynomials of $S^{(i)}$ which are regular with respect to ξ_i. (See [1, p. 71].) Denoting δ_{s-r} by $\rho^{(i)}$ and ϵ_1 by $\epsilon^{(i)}$, we conclude from **1** that $\prod_{j=1}^{r} \epsilon_j = \rho^{(i)} = \nu(Cl(L'_{i-1} \div L'_{i-1}))$, while $Cl(L'_{i-1}) = L'_{i-1}/(\rho^{(i)}) = L'_{i-1}/(\epsilon^{(i)})$ and finally $(\epsilon^{(i)}) = L'_{i-1}/Cl(L'_{i-1})$. (A scalar between parentheses denotes the ideal generated by that scalar.) It follows from Theorem 4.1 that $\rho^{(i)}$ and $\epsilon^{(i)}$ can also be considered as the generators of the highest dimensional non-zero determinantal factor and invariant factor respectively of $Cl(L_{i-1}) \div L_{i-1}$, and hence, $\rho^{(i)} = \nu(Cl(L_{i-1}) \div L_{i-1})$ and $(\epsilon^{(i)}) = L_{i-1}/Cl(L_{i-1})$. (See [1, p. 71].)

Let us now return to the scalar domain $S^{(i)}$ and again consider the variables $\xi_{i+1}, \cdots, \xi_n$ as not adjoined to $P(\gamma)$. The following definition is the same as for ideals (see [1, Definition VI, p. 71]):

Definition 5.1. *The polynomials $\rho^{(i)}$ and $\epsilon^{(i)}$ are called the i-th resultant and the i-th elementary divisor of the linear set L. The resultant ρ and the elementary divisor ϵ are then defined as $\rho = \prod_{i=1}^{n} \rho^{(i)}$ and $\epsilon = \prod_{i=1}^{n} \epsilon^{(i)}$.*

Theorem VIII in [1, p. 71] also holds for linear sets:

Theorem 5.1. *The product $\prod_{j=i}^{n} \rho^{(j)}$ can be divided by $\prod_{j=i}^{n} \epsilon^{(j)}$ and both these products are contained in $L/Cl_{i-1}(L)$. Consequently, for $i = 1$, the resultant ρ of a linear set L can be divided by the elementary divisor ϵ and both are contained in $L/Cl(L)$. Finally, a power of ϵ can be divided by ρ.*

Proof. The proof is the same as in [1, pp. 71-72] if we bear in mind that $Cl_0(L)$ is not necessarily the whole vector space as in the case of the ideals but is equal to the ordinary closure, $Cl(L)$, of L.

The next theorem was discussed in the introduction:

THEOREM 5. 2. *If the linear set L_1 contains the linear set L_2, then they are equal if and only if they have the same rank and the same resultant.*

Proof. As $L_2 \subseteq L_1$, we know that $Cl(L_2) \subseteq Cl(L_1)$. Since the ranks of L_1 and of L_2 are the same, we conclude that $Cl(L_2) = Cl(L_1)$ (see **1**), i. e. $Cl_0(L_2) = Cl_0(L_1)$. The proof then proceeds as for ideals. (See [1, Theorem IX, p. 72].)

In the corresponding theorem on ideals the rank is not mentioned since all ideals have the same rank, namely 1.

For a matrix $A = (\alpha_{ij})$, where the α_{ij} are elements of S and whose rows generate a transformed linear set, the resultant is defined as the resultant of that linear set. Considering only matrices whose rows generate transformed linear sets, we have the following immediate corollary of Theorem 5. 2:

THEOREM 5. 3. *A system of linear equations* $\sum_{i=1}^{s} \zeta_i \alpha_{ij} = \gamma_j$ $(j = 1, \cdots, m)$, *where the α_{ij} and γ_j are elements of S, can be solved simultaneously for elements of S if and only if the matrix $A = (\alpha_{ij})$ and the augmented matrix, which we obtain by adding the row $(\gamma_1, \cdots, \gamma_m)$ to A, have the same rank and the same resultant.*

The following theorem and its proof are word for word the same as in [1, p. 73]:

THEOREM 5. 4. *Let $\rho^{(i)} = \alpha^{(i)}\beta^{(i)}$ be a factorization of the i-th resultant of the linear set L into two relatively prime polynomials of $S^{(i)}$. Then, there exist two unique linear sets A and B which both contain L such that $Cl_{i-1}(A) = Cl_{i-1}(B) = Cl_{i-1}(L)$ while after adjunction of $\xi_{i+1}, \cdots, \xi_n$ to $P(\gamma)$, $\nu(Cl(L_{i-1}) \div A_{i-1}) = \alpha^{(i)}$ and $\nu(Cl(L_{i-1}) \div B_{i-1}) = \beta^{(i)}$. Furthermore, $Cl_i(L) = [A \frown B]$ and $A = Cl_i(L/(\beta^{(i)}))$ and $B = Cl_i(L/(\alpha^{(i)}))$.*

6. The resultant ρ and the ideal $L/Cl(L)$. A system of i elements $\bar{\xi}_1, \cdots, \bar{\xi}_i$ of the algebraic closure P' of $P(\gamma, \xi_{i+1}, \cdots, \xi_n)$ is called a root of dimension $n - i$ of an ideal $\mathfrak{a}$ of S if for $\xi_1 = \bar{\xi}_1, \cdots, \xi_i = \bar{\xi}_i$, $\xi_{i+1} = \xi_{i+1}, \cdots, \xi_n = \xi_n$, the polynomials of $\mathfrak{a}$ vanish. From the theory of elimination of $\mathfrak{a}$, as explained in [1, Chapter VI], we obtain the properties of the sequence of ideals $\mathfrak{a}_{n+1} \subseteq \cdots \subseteq \mathfrak{a}_1$, which is uniquely determined by $\mathfrak{a}$. If we then

take the ideal $L/Cl_{i-1}(L)$ as the ideal $\mathfrak{a}$, we prove in the same way as in [1, pp. 77-78] that the ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_i$ are different from the zero-ideal and that the i-th elementary divisor $\epsilon^{(i)}$ of L is a divisor of the highest common factor of the polynomials of $\mathfrak{a}_i$. Since this remains true if we first transform the variables by the special transformation, $\xi_i = -\alpha_1\xi_1 - \cdots - \alpha_{i-1}\xi_{i-1} + \zeta_i$ and adjoin the α's to $P(\gamma)$, and as furthermore a power of $\epsilon^{(i)}$ can be divided by the i-th resultant $\rho^{(i)}$ of L, Theorem XIII of [1, p. 78] holds for linear sets:

THEOREM 6.1. *Every root $\bar{\xi}_i \epsilon P'$ of the i-th resultant $\rho^{(i)}$ of the linear set L can be extended in a unique way into a root of dimension $n-i$ of $L/Cl_{i-1}(L)$, and consequently of $L/Cl(L)$. If we use the above special transformation, the polynomial $\rho^{(i)}$ is replaced by the polynomial $\bar{\rho}^{(i)}(\xi, \zeta)$ which can be factored in $P'(\alpha)$ as follows:*

$$\bar{\rho}^{(i)}(\xi, \zeta) = \prod \{\zeta_i - (\bar{\xi}_{ij} + \alpha_1\bar{\xi}_{1j} + \cdots + \alpha_{i-1}\bar{\xi}_{i-1,j})\}^{k_j}.$$

Here, $\bar{\xi}_{1j}, \cdots, \bar{\xi}_{ij}$ represent all the roots of dimension $n-i$ of $L/Cl_{i-1}(L)$, which we obtain in the above way from the linear factors of $\rho^{(i)}$. This factorization remains valid if the variables $\xi_{i+1}, \cdots, \xi_n$ are replaced by elements of $P(\gamma)$.

As $\rho = \prod_{j=1}^{n} \rho^{(j)} \equiv 0(L/Cl(L))$, every root of $L/Cl(L)$ is the extension of a root of one of the factors $\rho^{(i)}$ of ρ. Theorem 6.1 asserts the converse, namely that every root of a factor $\rho^{(i)}$ of ρ can be extended to a root of $L/Cl(L)$. Consequently the "main results" in the introduction are completely proved.

Theorem 5.4 asserts that the factorization of $\rho^{(i)}$ into powers of irreducible polynomials of $S^{(i)}$, $\rho^{(i)} = \prod_{j=1}^{t} \alpha_j^{s_j}$, gives rise to a unique decomposition $Cl_i(L) = [A^{(1)} \cap \cdots \cap A^{(t)}]$, such that after adjunction of $\xi_{i+1}, \cdots, \xi_n$ to $P(\gamma)$, $\nu(Cl(L_{i-1}) \div A^{(j)}_{i-1}) = \alpha_j^{s_j}$. Hence, the number of restclasses of the factor group $Cl(L_{i-1}) \div A^{(j)}_{i-1}$, which is independent with respect to the field $P(\gamma, \xi_{i+1}, \cdots, \xi_n)$, is equal to the multiplicity of the factor α_j of $\rho^{(i)}$. (See the Introduction and **1**.)

Finally, for the reasons explained in [1, p. 79], if the field P is infinite, the variables $\gamma_{i,j}$ can be specialized as elements of P in such a way that all the above results remain valid. Hence, in that case, the linear transformation $\eta = U(\xi)$, which was used to transform the linear sets into transformed linear sets, may be considered as a transformation with coefficients in the field P.

REFERENCES.

1. K. Hentzelt and E. Noether, "Zur Theorie der Polynomideale und Resultanten," *Mathematische Annalen*, vol. 88 (1922), pp. 53-79.

2. E. Steinitz, "Rechteckige Systeme und Moduln in algebraischen Zahlkörpern I," *Mathematische Annalen*, vol. 71 (1912), p. 340.

3. E. Snapper, "Structure of Linear Sets," *Transactions of the American Mathematical Society*, vol. 52 (1942), pp. 258-259.

4. H. Fitting, "Die Determinantenideale eines Moduls," *Jahresberichte der Deutschen Mathematiker Vereinigung*, vol. 46 (1936), p. 197.

5. R. Dedekind, "Über einen arithmetischen Satz von Gauss," *Dedekind Gesammelte mathematische Werke* II (1931), pp. 35-38.

PRINCETON UNIVERSITY,
PRINCETON, N. J.

r-REGULAR CONVERGENCE SPACES.*

By PAUL A. WHITE.

In most previous work on hyperspaces such as the space of all closed subsets or of all continua in a given space M, the well known Hausdorff metric has been used. In this work the hyperspace K^r of lc^r closed subsets of a compact metric space M, where r is an arbitrary integer, is considered. (See Definition 1.2). It is easily seen that the Hausdorff metric, which makes the limit concept in the hyperspace correspond to ordinary point set convergence in the original space, is not desirable here. For example, K^r would not be closed in the space of all closed subsets of M. However G. T. Whyburn has introduced the notion of regular convergence (see Definition 1.1) which does require that the limit set be lc^r. The major part of this work is devoted to establishing a metric in K^r where regular convergence is used to define the limit concept in K^r.

After the main part of this work was completed it was learned that S. Mazurkiewicz [1] had considered the hyperspace of locally connected subcontinua of a locally connected compact metric space M. This is what is called the set $K_1{}^0$ in this work where $r = 0$ (see Definition 7.2). Also we require only that M be a compact metric space. It is interesting to note that the limit notion used by Mazurkiewicz is equivalent to ours although phrased differently. It should be mentioned however that his metric is complete whereas ours is only complete in very special cases. In this respect his is more desirable than ours although defined in a more restricted space.

A large part of the work is devoted to finding rather general topological properties of K^r. Some time is spent in considering what special properties K^r will have if M is specialized and conversely. It is found that very general hypotheses on K^r or $K_1{}^0$ demand very special kinds of spaces for M. It is hoped that through the study of K^r many properties can be deduced that could not be obtained from the usual hyperspaces. This hope is based on the fact that not so many properties of the original space are carried over to our hyperspace as is true in the case of the usual ones. Thus many more essentially different things can arise in the hyperspace that did not appear in the original space. For example, the hyperspace almost always has more com-

* Received June 14, 1942.

[1] *Fundamenta Mathematicae*, vol. 24 (1935), pp. 118-134.

ponents than the original space. Thus certain collections of subsets are seen to be related that might not have been seen previously.

1. The definition of convergence and the L^* axioms. In this entire work, we shall assume that our space M is compact and metric. All of our ordinary complexes and cycles shall have modulus two coefficients and the Vietoris cycles used shall consist of these as coördinate cycles. A knowledge of the definitions and fundamental properties concerning Vietoris cycles will be assumed and the words "complete cycle" or just "cycle" will be used throughout to mean "Vietoris cycle." For a treatment of these combinatorial concepts reference is made to the original paper of Vietoris.[2]

DEFINITION 1.1. The sequence of closed sets $[A_i]$ will be said to *converge r-regularly* to A, provided $[A_i]$ converges to A $([A_i] \rightarrow A)$, and that for every $\epsilon > 0$ there shall exist a $\delta > 0$ and an N such that if $n > N$, any r-dimensional cycle in A_n of diameter $< \delta$ is homologous to 0 (~ 0) in a subset of A_n of diameter $< \epsilon$. (By the diameter of a complete cycle, we mean the smallest diameter of a carrier of the cycle. A carrier of a cycle V is a closed set P such that V is a cycle of P.)

DEFINITION 1.2. A closed set A is said to be *locally γ^r-connected* $(r - lc)$ provided that for every $\epsilon > 0$ there shall exist a $\delta > 0$ such that every r-dimensional cycle of A of diameter $< \delta$ is homologous to 0 in a subset of A of diameter $< \epsilon$. A closed set is lc^r if it is $s - lc$ for all s, $(0 \leqq s \leqq r)$.

Notation. We shall denote by H the hyperspace of all closed subsets of M, and by K^r the hyperspace of all closed subsets that are lc^r. We shall think of r as arbitrary but fixed until otherwise stated, so that we shall write K instead of K^r henceforth. A capital letter will denote a closed subset constituting an element of K, and the same small letter will denote the point of K corresponding to this set. The symbol "$\underset{r}{\rightarrow}$" shall denote r-regular convergence, and "$\underset{\leqq r}{\rightarrow}$" shall denote s-regular convergence for all $s \leqq r$. $\delta(A)$ shall denote the diameter of the set A and $U_\epsilon(A)$ shall denote the set of all points whose distance from some point in A is $< \epsilon$. Finally $\dot{C}$ shall denote the boundary of the complex C.

DEFINITION 1.3. The sequence $[p_i]$ in H shall be said to *converge to a limit* p in H $([p_i] \rightarrow p)$, if and only if $[P_i] \underset{\leqq r}{\rightarrow} P$.

THEOREM 1.1. *Any infinite subsequence of a convergent sequence in H is a convergent sequence with the same limit.*

---

[2] Vietoris, *Mathematische Annalen*, vol 97 (1927), pp. 454-472.

The proof is a direct application of the definition of convergence.

THEOREM 1.2. *If $p_i = p$ for all i, then $[p_i] \to p$ if and only if P is lc^r.*

Proof. Clearly the definitions of s-regular convergence and locally γ^s-connectedness coincide when $p_i = p$ for all i; hence the theorem.

THEOREM 1.3. *Each point of H will converge to itself in the sense of Theorem 1.2, if and only if M is finite.*

Proof. The sufficiency follows immediately from Theorem 1.2, for if M is finite then every subset is both closed and lc^r.

Conversely, suppose that H has the property of the theorem, but that M is infinite. Since M is compact there exists an infinite convergent sequence of distinct points $[P_i] \to P$. Let A be the closed set $[P_i] + P$. By Theorem 1.2 A should be lc^r, but it is not since $P_i + P$ $(i = 1, 2, \cdots)$ is a sequence of 0-cycles whose diameters converge to 0, but which do not bound in A.

COROLLARY 1.21. *Every point of K converges to itself in the sense of Theorem 1.2.*

Proof. The proof follows immediately from the definition of K and Theorem 1.2.

Note. Theorem 1.3 and Corollary 1.21 make it seem wise to abandon the study of H in general and restrict ourselves only to K.

THEOREM 1.4. *If $[p_i]$ in H does not converge to p, there exists an infinite subsequence $[p_{n_i}]$ such that no subsequence of it converges to p.*

Proof. Case 1. $[P_i] \to P$ but not s-regularly for some $s \leqq r$. This means there exists an $\epsilon > 0$ such that for any $\delta > 0$ and N, there is an $n > N$ and a complete s-dimensional cycle $\gamma_n{}^s$ in P_n with $\delta(\gamma_n{}^s) < \delta$ but $\gamma_n{}^s$ not homologous to 0 in a subset of P_n of diameter $< \epsilon$. Pick $[\delta_i] \to 0$ and $[N_i] \to \infty$, and let $n_i > N_i$ be chosen as above. Now the sequence $[P_{n_i}]$ clearly contains no s-regular convergent subsequence so that $[p_{n_i}]$ has no convergent subsequence.

Case 2. $[P_i]$ does not converge to P. Since M is compact there exists an $\epsilon > 0$ and an infinite subsequence $[P_{n_i}]$ such that each P_{n_i} has the property that either $P \notin U_\epsilon(P_i)$ or $P_i \notin U_\epsilon(P)$. Clearly no subsequence of $[P_{n_i}]$ converges to P and hence no subsequence of $[p_{n_i}]$ converges to p.

THEOREM 1.5. *K is an L^*-space of Kuratowski.*

Proof. Kuratowski has given the name "L^*-space" to any space in which a convergence notion is defined such that the properties in Theorems 1.1, 1.21, and 1.4 hold.

2. Open sets and their relation to the limit concept. Henceforth we shall consider only the space K and all notions such as complement of a set E (denoted by $C(E)$) will be relative to K unless otherwise stated.

DEFINITION 2.1. We shall call p a *limit point* of the set E contained in H provided there exists an infinite sequence of distinct points of E converging to p as a limit.

DEFINITION 2.2. A set is *closed* if it contains all of its limit points.

DEFINITION 2.3. A set is *open* if its complement is closed.

The following lemmas, which we now prove, will be useful in proving the following theorems.

LEMMA 2.1. *If A is lc^{r-1}, then for every set of numbers ϵ, d, η, ρ such that $\epsilon > d > 0$, $\eta > 0$, $\rho > 0$ there exists a $\delta > 0$, such that for every δ-cycle C^r of A of diameter $< d$, there is a complete cycle $D^r = (D_1{}^r, D_2{}^r, \cdots)$ of diameter $<$ minimum $(3d, \epsilon)$ such that $D_j{}^r \underset{\eta}{\sim} C^r$ for all j in an ϵ-subset of A. Also this homology takes place in the ρ-neighborhood of C^r, which therefore contains D^r.*

Proof. This lemma follows directly from Lemma 1 of a paper by R. L. Wilder.[3] If we choose $\alpha < \eta$, $(\epsilon - d)/2$, d, ρ then by that lemma there exists a number $\delta > 0$ such that every δ-simplex has a Vietoris chain realization of diameter $< \alpha$. It follows from the definition given in that paper that when we add these realizations for all simplices of C^r (taking subsequences when necessary), we obtain a Vietoris cycle $D^r = (D_1{}^r, D_2{}^r, \cdots)$ which clearly has diameter $< d + 2\alpha < d + 2d = 3d$, or $d + 2(\epsilon - d)/2 = \epsilon$. Also by using the prism construction,[4] we see that for each j, $D_j{}^r \underset{\alpha}{\sim} C^r$; hence $D_j{}^r \underset{\eta}{\sim} C^r$. Finally we recall that the prism construction requires no new vertices; hence the homology occurs in the α and hence the ρ-neighborhood of C^r.

LEMMA 2.2. *If $[A_i] \to A$, where each A_i is closed, and $e > 0$, $d > 0$ are numbers such that if $\gamma^s \subset A$ is a complete cycle of diameter $\leqq d$, then $\gamma^s \sim 0$ in a subset of A of diameter $< e$, then for any $\epsilon > 0$ there is a $\delta > 0$,*

---

[3] R. L. Wilder, *Duke Mathematical Journal*, vol. 1 (1935), p. 546.

[4] Alexandroff-Hopf, *Topologie*, p. 199.

$e_1 < e$, and N such that if $n > N$, any s-dimensional δ-cycle in A_n of diameter $\leqq d$ is $\underset{\epsilon}{\sim} 0$ in an e_1-subset of A_n.[5]

Proof. If the lemma were false, then for some $\epsilon > 0$, there would exist sequences $[\delta_i] \to 0$, $[e_1{}^i] \to 0$, $[N_i] \to \infty$, and a δ_i-cycle $C_i{}^s$ in A_{N_i} of diameter $\leqq d$ which is not ϵ-homologous to 0 in a subset of A_{N_i} of diameter $< e_1{}^i$. Pick a convergent subsequence of the point sets $[C_i{}^s]$ converging to a limit set C in A. $\delta(C_i{}^s) \leqq d$ for all i, hence $\delta(C) \leqq d$. We can further suppose that the subsequence $[C_i{}^s]$ was so chosen that $U_{\delta_i}(C_i) \supset C$, and $U_{\delta_i}(C) \supset C_i$ for all i. Let $C_i = (x_0, x_1, \cdots, x_g)$, where the x_i are the vertices of C_i. For each $j \leqq g$, let y_j be a point of C such that $\rho(x_j, y_j) < \delta_i$. For each simplex $(x_{i_0}, x_{i_1}, \cdots, x_{i_s})$ in C_i, let $(y_{i_0}, y_{i_1}, \cdots, y_{i_s})$ be a simplex and let $D_i{}^s$ be the cycle composed of all these simplexes.[6] Clearly $D_i{}^s$ is a $3\delta_i$-cycle and $\delta(D_i{}^s) \leqq d$. Since C is compact and the meshes $[3\delta_i] \to 0$, we can pick a subsequence of the $[D_i{}^s]$ so as to form a Vietoris cycle. Call this cycle $D^s = (D_1{}^s, D_2{}^s, \cdots)$. By hypothesis $D^s \sim 0$ in a subset of A of diameter $< e$. That is, $D^s \sim 0$ in a subset whose diameter e' is $< e$. Hence there is an N' such that if $i > N'$, $D_i{}^s = \dot{E}_i{}^{s+1}$, where $E_i{}^{s+1}$ is an $\epsilon/3$-complex and $\delta(E_i{}^{s+1}) \leqq e'$. Pick k such that $e - e_1{}^k < (e - e')/3$, $k > N'$ and $\delta_k < (2(e - e')/9, \epsilon/3)$. Project $E_k{}^{s+1}$ into A_k, keeping vertices of $C_k{}^s$ fixed. Let the resultant complex be $F_k{}^{s+1}$. $\delta(F_k{}^{s+1}) < e' + 3 \cdot (2/9)(e - e') = e' + (2/3)(e - e')$. But $e - e_1{}^k - e' < (e - e')/3 - e'$, or $(2/3)(e - e') + e' < e$, and $\delta(F_k{}^{s+1}) < e_1{}^k$. Also $F_k{}^{s+1}$ is an $\epsilon/3 + 2 \cdot (\epsilon/3) = \epsilon$-complex, and $\dot{F}_k{}^{s+1} = C_k{}^s$. But this says that $C_k{}^s \underset{\epsilon}{\sim} 0$ in a subset of A of diameter $< e_1{}^k$ contrary to our assumption; hence the lemma must be true.

LEMMA 2.3. *If $[A_i] \underset{\leqq r}{\to} A$, where each A_i is closed and lc^{r-1}, and $\epsilon > \delta_r > 0$ are numbers such that every complete r-dimensional cycle γ^r in A with $\delta(\gamma^r) \leqq \delta_r$ is homologous to 0 in a subset of A of diameter $< \epsilon$, then for every $\sigma > 0$ there is an N such that if $i > N$ and γ^r is a complete r-dimensional cycle of A_i of diameter $\leqq \delta_r$, then $\gamma^r \sim 0$ in a subset of A_i of diameter $< \epsilon + \sigma$.*

Proof. Suppose the lemma is false, then there is a $\sigma > 0$, a sequence $[n_i] \to \infty$, and a sequence of complete cycles $[\gamma_i{}^r]$ in $[A_{n_i}]$ such that $\delta(\gamma_i{}^r) \leqq \delta_r$, but $\gamma_i{}^r$ is not homologous to 0 in a subset of A_{n_i} of diameter $< \epsilon + \sigma$. Thus if $\gamma_i{}^r = (C_{i1}, C_{i2}, \cdots)$ then for each i there is a number $\eta_i > 0$ such that for only a finite number do we have $C_{ij} \underset{\eta_i}{\sim} 0$ in a subset of A_{n_i}

[5] This is a modification of Lemma (1.2), G. T. Whyburn, *Fundamenta Mathematicae*, vol. 25 (1935), p. 410.

[6] We shall call a complex $D_i{}^s$ obtained this way, a *δ_i-projection* of C_i in C.

of diameter $< \epsilon + \sigma$. We can omit this finite number and suppose that γ_i^r consists of only the remainder.

The r-regular convergence tells us that there are positive numbers N_r and $d_r < \sigma/4$ such that if $n > N_r$ and if γ^r is a complete cycle of A_n of diameter $< 3d_r$, then $\gamma^r \sim 0$ in a subset of A_n of diameter $< \sigma/4$. Inductively for each $d_j > 0$ and $j = r, r-1, \cdots, 1$ there is a $d_{j-1} < d_j$ and a number N_{j-1} such that if $n > N_{j-1}$ and if γ^{j-1} is a cycle of A_n of diameter $< 3d_{j-1}$, then $\gamma^{j-1} \sim 0$ in a subset of A_n of diameter $< d_j$. Now in Lemma 2.2 let $d = \delta_r$, $e = \epsilon$, and $\epsilon = d_0$; then the conclusion is that there are numbers N', $\delta < \delta_r$, and $\epsilon_1 < \epsilon$ such that for $n > N'$ any r-dimensional δ-cycle in A_n of diameter $\leqq \delta_r$ is d_0-homologous to 0 in a subset of A_n of diameter $< \epsilon_1$.

Choose $N = N' + \sum_{i=0}^{r} N_i$ and consider any $n_t > N$. In Lemma 2.1 let $A = A_{n_t}$, $\epsilon = \epsilon$, $d = (\delta_r + \epsilon)/2$, $\eta = \eta_t$, $\rho = \sigma/2$; then the conclusion tells us there is a $\delta' > 0$ such that for any δ'-cycle C^r of A_{n_t} of diameter $< (\delta_r + \epsilon)/2$, there is a complete cycle $D^r = (D_1^r, D_2^r, \cdots)$ of diameter $< \epsilon$ such that $D_j^r \underset{\eta_t}{\sim} C^r$ for all j in a subset of A_{n_t} of diameter $< \epsilon$ and that the homology occurs in the $\sigma/2$-neighborhood of C^r. Since $\gamma_t^r = (C_{t1}, C_{t2}, \cdots)$ is a complete cycle, we can find a C_{tk}^r which is both a δ and a δ'-cycle. Also by hypothesis $\delta(C_{tk}^r) \leqq \delta_r < (\delta_r + \epsilon)/2$. Since C_{tk}^r is a δ-cycle $C_{tk}^r = \dot{E}^{r+1}$ where E^{r+1} is a d_0-complex of diameter $< \epsilon_1$. Since C_{tk}^r is also a δ'-cycle, we can find a complete cycle $D^r = (D_1^r, D_2^r, \cdots)$ such that $D_j^r \underset{\eta_t}{\sim} C_{tk}^r$ in a subset of A_{n_t} of diameter $< \epsilon$ and that $D_j^r \subset$ the $\sigma/2$-neighborhood of C_{tk}^r.

Since E^{r+1} is a d_0-complex, it is clear by the choice of the numbers d_j that a Vietoris chain realization of E^{r+1} can be constructed.[7] Furthermore since $\dot{E}^{r+1} = C_{tk}^r$ the realization of C_{tk}^r as a Vietoris cycle $D^r = (D_1^r, D_2^r, \cdots)$, as concluded in Lemma 2.1, can be carried out simultaneously with that of E^{r+1} in such a way that the realization of each simplex of C_{tk}^r is used in the realization of the $(r+1)$-dimensional simplices of E^{r+1} to which it belongs. Let $\gamma^{r+1} = (E_1^{r+1}, E_2^{r+1}, \cdots)$ be the V-chain realization of E^{r+1}, which will have diameter $< \epsilon_1 + 2(\sigma/4) = \epsilon_1 + \sigma/2$. Furthermore the simultaneous realizations imply $\dot{E}_j^{r+1} = D_j^r$ for all j where $\delta(E_j^{r+1}) < \epsilon_1 + \sigma/2$. We can pick j such that E_j^{r+1} is an η_t-complex, then $D_j^r \underset{\eta_t}{\sim} 0$ in a subset of A_{n_t} of diameter $< \epsilon_1 + \sigma/2$. Also $D_j^r \underset{\eta_t}{\sim} C_{tk}^r$ in a subset of A_{n_t} in the $(\sigma/2)$-neighborhood of C_{tk}^r. Therefore $C_{tk}^r \underset{\eta_t}{\sim} 0$ in a subset of A_{n_t} of diameter $< \epsilon_1 + \sigma/2 + \sigma/2 = \epsilon_1 + \sigma < \epsilon + \sigma$. But this is contrary to the definition of γ_t^r and the lemma is proved.

---

[7] See reference [3], p. 545.

LEMMA 2.4. *If* $[P_{ij}] \underset{\leqq r}{\rightarrow} P_i$, $[P_i] \underset{\leqq r}{\rightarrow} P$ *where each* P_{ij} *is closed and* lc^{r-1}, *then there is a diagonal sequence of the* $[P_{ij}]$ *which converges t-regularly to* P *for all* $t \leqq r$.

Proof. It will first be useful to generalize Lemma 2.3 by applying it for all $s \leqq r$. That is, if $\epsilon > \delta_s > 0$ are numbers such that every complete cycle in A of diameter $\leqq \delta_s$ bounds in a subset of A of diameter $< \epsilon$, then for any $\sigma > 0$ there is an N_s such that if $i > N_s$ and $\gamma_i{}^s$ is a complete s-dimensional cycle in A with $\delta(\gamma^s) \leqq \delta_s$, then $\gamma_i{}^s \sim 0$ in a subset of A_i of diameter $< \epsilon + \sigma$. Let $\delta =$ minimum $(\delta_0, \delta_1, \cdots, \delta_r)$ and $N = \sum_0^r N_s$; then if $i > N$ and γ is any complete cycle in A_i of dimension $\leqq r$ and diameter $\leqq \delta$, we have $\gamma \sim 0$ in a subset of A_i of diameter $< \epsilon + \sigma$.

Since $[P_i] \underset{\leqq r}{\rightarrow} P$, we can find for each $\epsilon_k > 0$ in a sequence $[\epsilon_k] \rightarrow 0$, numbers $\delta_k > 0$ and N_k such that if $i > N_k$ and $\gamma^s \subset P_i$ is a complete cycle of diameter $\leqq \delta_k$ for any $s \leqq r$, then $\gamma^s \sim 0$ in a subset of P_i of diameter $< \epsilon_k$. By the above generalization of Lemma 2.3, if $\sigma = \epsilon_k$ there is a number $M_i{}^k$ for each $i > N_k$ such that if $j > M_i{}^k$ and γ^s is a complete cycle in P_{ij} for any $s \leqq r$ with diameter $\leqq \delta_k$, then $\gamma^s \sim 0$ in an $(\epsilon_k + \epsilon_k) = 2\epsilon_k$-subset of P_{ij}. Also there are numbers $R_i{}^k$ such that if $j > R_i{}^k$ then $U_{\epsilon_k}(P_i)$ contains P_{ij}, and $U_{\epsilon_k}(P_{ij})$ contains P_i. For each i, $N_k < i \leqq N_{k+1}$, pick a number $n_i = \sum_{m=1}^k R_i{}^m + \sum_{m=1}^k M_i{}^m$. $[P_{in_i}] \underset{\leqq r}{\rightarrow} P$, for if we consider any $\epsilon > 0$ there is a number $\bar{n}$ such that $\epsilon_{\bar{n}} < \epsilon/2$. Let $\delta = \delta_{\bar{n}}$. If $i > N_{\bar{n}}$, then $n_i > R_i{}^{\bar{n}}$, $U_\epsilon(P_i)$ contains P_{in_i}, and $U_\epsilon(P_{in_i})$ contains P_i since $\epsilon_{\bar{n}} < \epsilon/2$. Also since $n_i > N_i{}^{\bar{n}}$ we know that if γ^s is any complete cycle in P_{in_i} for any $s \leqq r$ of diameter $< \delta$, then $\gamma^s \sim 0$ in a subset of P_{in_i} of diameter $< 2 \cdot \epsilon_{\bar{n}} < 2 \cdot (\epsilon/2) < \epsilon$. The first of these statements implies that $[P_{in_i}] \rightarrow P$, while the second implies that the convergence is t-regular for all $t \leqq r$.

THEOREM 2.5. *For any set* $E \subset K$; E' (*and hence* $\bar{E}$) *is closed.*

Proof. Consider any point p in $(E')'$. By the definition of a limit point, there exists a sequence $[p_i]$ of distinct points in E' such that $[p_i] \rightarrow p$. Since $p_i \in E'$, there is a sequence $[p_{ij}]$ of distinct points such that $[p_{ij}] \rightarrow p_i$. That is to say, $[P_i] \underset{\leqq r}{\rightarrow} P$, $[P_{ij}] \underset{\leqq r}{\rightarrow} P_i$; hence by Lemma 2.4 there is a diagonal sequence $[P_{in_i}] \underset{\leqq r}{\rightarrow} P$ or $[p_{in_i}] \rightarrow p$ where $[p_{in_i}]$ is in E and may be assumed to consist of distinct points. This means p is a limit point of E and E' is closed.

THEOREM 2.6. *A necessary and sufficient condition that p be a limit point of a set E is that every open set containing p shall contain at least one point of E different from p.*

Proof. To prove the necessity suppose that p is in E'. Then there exists a sequence of distinct points $[p_i] \to p$, such that each $p_i \in E$ and $p_i \neq p$ for all i. Now suppose that there is an open set U containing p, but containing no point of E different from p. In particular $[p_i] \subset C(U)$ which is closed, and hence contains p contrary to the assumption that p is in U.

Conversely, suppose that every open set containing p contains a point of E distinct from p, but that $p \notin E'$. That is, there does not exist an infinite sequence of distinct points of E converging to p. This implies that $p + C(\bar{E})$ is open, for $C(p + C(\bar{E})) = C(p) \cdot \bar{E}$ is closed since $\bar{E}$ is closed by Theorem 2.5 and p is not a limit point of E'. Thus $p + C(\bar{E})$ is an open set containing p, but not containing any point of E distinct from p, contrary to the hypothesis. Hence $p \in E'$, which concludes the sufficiency proof.

3. The Hausdorff axioms.

THEOREM 3.1. *The space K is closed in H (in fact $H' \subset K$).*

Proof. This theorem is a direct consequence of a theorem of G. T. Whyburn,[8] for consider a sequence $[p_i]$ in H such that $[p_i] \to p$. This means that $[P_i] \underset{\leqq r}{\to} P$, where the $[P_i]$ are all closed, but the above mentioned theorem states that under these conditions P is closed and lc^r, or p is in K. Thus, in particular, $H' \subset K$, and K is closed in H.

THEOREM 3.2. *K is open (in H).*

Proof. The complement of K is the null set which is closed; hence K is open.

THEOREM 3.3. *The product of any two open sets is open.*

Proof. Evidently it is sufficient to prove that the sum of two closed sets is closed. This follows from the fact that a limit point of the sum of two sets C_1, C_2 is by Definition 2.1 the limit of an infinite sequence of distinct points of $C_1 + C_2$ and hence, by virtue of Theorem 1.1, a limit point of C_1, say.

DEFINITION 3.1. If $A \subset M$, then by $h_k(A)$ we mean the subset of K corresponding to all subsets of A which are closed and lc^r.

[8] *American Journal of Mathematics*, vol. 57 (1935), p. 904.

THEOREM 3.4. *If A is open, so is $h_k(A)$.*

Proof. If the theorem were false, then there would be a point p in $h_k(A)$ and a sequence $[p_i]$ in the complement of $h_k(A)$ converging to p. This means that P is in A and $[P_i] \underset{\leqq r}{\rightarrow} P$, but $P_i \cdot C(A) \neq 0$ for all i. But $C(A)$ is compact, hence $\lim P_i = P$ intersects $C(A)$ contrary to the assumption that P is in A.

THEOREM 3.5. *If A is closed, so is $h_k(A)$.*

Proof. Let p be any limit point of $h_k(A)$. By definition there exists a distinct sequence $[p_i]$ of points of $h_k(A)$ converging to p. This implies that $[P_i] \underset{\leqq r}{\rightarrow} P$ where each P_i is in A. By the compactness of A, this implies that P is in A, and hence $p \subset h_k(A)$. Thus $h_k(A)$ is closed.

THEOREM 3.6. *If p and q are distinct, then there exist disjoint open sets U_p and U_q, containing p and q respectively.*

Proof. Since p and q are distinct, we can suppose that $Q \not\subset P$. Then there exists an $\epsilon > 0$ such that $\overline{U_\epsilon(P)}$ does not contain Q; hence $q \epsilon$ the complement of $h_k(\overline{U_\epsilon(P)}) = U_q$. By Theorem 3.5 $h_k(\overline{U_\epsilon(P)})$ is closed; hence its complement U_q is open. By Theorem 3.4 $h_k(U_\epsilon(P)) = U_p$ is open and it contains p. Clearly U_p and U_q are disjoint and therefore fulfill the requirements of the theorem.

THEOREM 3.7. *If "neighborhood" is interpreted to mean "open set," then K is a Hausdorff space.*

Proof. The proof follows immediately from Theorems 3.2, 3.3 and 3.6.

4. Regularity.

THEOREM 4.1. *For any point p and $\epsilon > 0$, the subset of K consisting of all points of K corresponding to sets of M whose ϵ-neighborhoods contain P is open.*

Proof. Suppose that the theorem is false for some point p and $\epsilon > 0$. Then the set described in the theorem contains a limit point q of its complement. That is, $U_\epsilon(Q)$ contains P, but there exists a sequence $[Q_i] \underset{\leqq r}{\rightarrow} Q$ such that P is not contained in the ϵ-neighborhood of Q_i for each i. P and Q are compact; hence there exists a farthest point x of P from Q and $d = \rho(x, Q)$

$< \epsilon$. This implies that $U_{(\epsilon+d)/2}(Q)$ contains P. But the convergence of $[Q_i]$ to Q implies that there is a number N such that $U_{(\epsilon-d)/2}(Q_N)$ contains Q, and hence $U_{(\epsilon-d)/2+(\epsilon+d)/2}(Q_N)$ contains P, or $U_\epsilon(Q_N)$ contains P, which contradicts the above assumption on Q_N and P.

Definition 4.1. If $P \subset M$ and $\epsilon > 0$, by $A_{\epsilon,p}$ we shall mean all points of K corresponding to sets Q in M such that $U_\epsilon(Q)$ contains P, $U_\epsilon(P)$ contains Q.

Corollary 4.11. *For every point p and $\epsilon > 0$, $A_{\epsilon,p}$ is open.*

Proof. By Theorem 3.4 $h_K(U_\epsilon(P))$ is open. Also the set O defined in Theorem 4.1 is open. The set $A_{\epsilon,p} = O \cdot h_K(U_\epsilon(P))$, and is open by Theorem 3.3.

Definition 4.2. The set of points p of K with the property that any complete s-dimensional cycle γ^s in P with diameter less than δ is homologous to zero in a subset of ρ of diameter less than ϵ, will be denoted by $K^s{}_{\epsilon,\delta}$.

The sets $K^s{}_{\bar{\epsilon},\delta}$, $K^s{}_{\epsilon,\bar{\delta}}$, $K^s{}_{\bar{\epsilon},\bar{\delta}}$ will be defined similarly where $\bar{\epsilon}$ means that $\leqq \epsilon$ replaces $< \epsilon$, etc.

Definition 4.3. $K_{\epsilon,\delta} = \prod_{s \leqq r} K^s{}_{\epsilon,\delta}$, etc.

Theorem 4.2. *$K^s{}_{\bar{e},d}$ is closed for all $d > 0$, $e > 0$, and $s \leqq r$.*

We first prove two lemmas.

Lemma 4.3. *If $[A_i]$ is a sequence of closed sets converging to A, and $e > 0$, $d > 0$ are numbers such that for every $\epsilon > 0$ there exists a $\delta > 0$ and an N such that if $n \geqq N$, any s-dimensional δ-cycle in A_n of diameter $< d$ is ϵ-homologous to 0 in a subset of A_n of diameter $\leqq e$, then any complete s-dimensional cycle in A of diameter $< d$ is homologous to 0 in a subset of A of diameter $\leqq e$.*[9]

Proof. Let $\gamma^s = (C_1, C_2, \cdots)$ be any complete s-dimensional cycle in A of diameter $< d$, and let d' be any number such that $\delta(\gamma^s) < d' < d$. We have to show that for any $\epsilon > 0$, there exists an integer M such that for $k > M$, $C_k \underset{\epsilon}{\sim} 0$ in a subset of A of diameter $\leqq e$. By hypothesis, given $\epsilon/4$, there exist positive numbers $\delta < \epsilon$ and N such that for any $n > N$, any s-dimensional δ-cycle in A_n of diameter $< d$ is $\underset{\epsilon/4}{\sim} 0$ in a subset of A_n of diameter $\leqq e$. Let us take M such that for $k > M$, C_k is a $\delta/3$-cycle; and with k fixed and $> M$,

[9] This is a modification of Lemma (1.1) of G. T. Whyburn, see footnote [8].

let $C_k = (x_0, x_1, \cdots, x_g)$, where the x_i are the vertices of C_k. Take an integer I such that for $i > I$, we have $A_i \subset U_{\delta'}(A)$ and $A \subset A_{\delta'}(A_i)$ where $\delta' = \min. (\delta/3, [d - d']/2)$. Take a fixed $j > I + N$ and δ'-project[10] C_k into $C^*_j = (y_0, y_1, \cdots, y_g)$, where y_t is the projection of x_t.

Now since $\rho(y_t, y_m) \leqq \rho(y_t, x_t) + \rho(x_t, x_m) + \rho(x_m, y_m) < \delta' + \delta/3 + \delta' \leqq \delta$, it follows that C^*_j is a δ-cycle. Also since $\rho(y_t, y_m) \leqq \delta' + d' + \delta' < (d - d')/2 + d' + (d - d')/2 = d$, then C^*_j is of diameter $< d$. Thus by hypothesis there exists an $\epsilon/4$-complex $Z^{s+1} = (z_0, z_1, \cdots, z_n)$ in A_j of diameter $\leqq e$ bounded by C^*_j. Project Z^{s+1} into a complex K^{s+1} in A by a δ'-projection. Then clearly K^{s+1} is an $(\epsilon/4 + 2\delta' < \epsilon/4 + 2\delta/3 < \epsilon/4 + 2\epsilon/3 = 11\epsilon/12)$-complex in A of diameter $\leqq e + 2(d - d')/2 = e + d - d'$. Thus $C_k \underset{11\epsilon/12}{\sim} 0$ in a subset of A of diameter $\leqq e + d - d'$, for any $k > M$. We note that d' was an arbitrary number $(\delta(\gamma^s) < d' < d)$ and that the choice of M did not depend on our choice of d'; therefore we can assert the above statement for $k > M$ where $d - d'$ is arbitrarily small. We shall show that this implies $C_k \underset{\epsilon}{\sim} 0$ in a subset of A of diameter $\leqq e$. To this end pick a sequence $[d'_i]$ such that $[d - d'_i] \to 0$. There exist $[K_i^{s+1}]$, each $11\epsilon/12$-complexes such that $\dot{K}_i^{s+1} = C_k$ and $\delta(K_i^{s+1}) \leqq d - d'_i + e$. Suppose that the sequence $[d'_i]$ was so chosen that the point sets making up the complexes $[K_i^{s+1}]$ converge to a point set K, which must clearly contain C_k and have diameter $\leqq e$. Pick an integer i such that $U_{\epsilon/24}(K)$ contains K_i. Now let K^{s+1} be the $\epsilon/24$-projection of K_i^{s+1} into K with points of C_k fixed. Clearly $\dot{K}^{s+1} = C_k$ and $\delta(K^{s+1}) \leqq e$, also K^{s+1} is an $(11\epsilon/12 + \epsilon/24 + \epsilon/24 = \epsilon)$-complex. That is, $C_k \underset{\epsilon}{\sim} 0$ in a subset of diameter $\leqq e$, and our lemma is proved.

LEMMA 4.4. *If $[A_i]$ is a sequence of closed sets converging $\leqq r$-regularly to A, and $e > 0$, $d > 0$ are numbers such that every complete s-dimensional cycle γ^s $(0 \leqq s \leqq r)$ of diameter $< d$ is ~ 0 in a subset of A_i of diameter $\leqq e$ for $i > N'$, then for any numbers $0 < d' < d$, $\epsilon > 0$, $\eta > 0$ there exists a number N such that if $n > N$ and C^s is any δ-cycle in A_n of diameter $< d'$ then $C^s \underset{\epsilon}{\sim} 0$ in a subset of A_n of diameter $< e + \eta$.*

Proof.[11] Let $\epsilon > 0$, $\eta > 0$, $d' > 0$ be given and let $\delta_s = \min. (\epsilon, d, \eta, [d - d']/2)$. By virtue of the $(s - 1)$-regular convergence, there exist positive numbers δ_{s-1} and N_{s-1} such that if $n > N_{s-1}$, then any γ^{s-1} in A_n of diameter $< 3\delta_{s-1}$ is ~ 0 in a subset of A_n of diameter $< \delta_s$. Likewise, by

---

[10] See footnote [6].

[11] This proof is a modification of the proof used in Theorem 1 of the paper referred to in footnote [8].

virtue of the $(s-2)$-regular convergence, using δ_{s-1}, we have positive numbers δ_{s-2} and N_{s-2} such that if $n > N_{s-2}$, then any γ^{s-2} in A_n of diameter $< 3\delta_{s-2}$ is ~ 0 in a subset of A_n of diameter $< \delta_{s-1}$. Continuing as in Lemmas 2. 1 and 2. 3 by the same argument, we reach numbers δ_0 and N_0 such that if $n > N$, then any γ^0 in A_n of diameter $< 3\delta_0$ is ~ 0 in a subset of A_n of diameter $< \delta_1$. We may suppose $\delta_s > \delta_{s-1} > \cdots \delta_0$. Let $\delta = \delta_0$ and $N = \sum_0^s N_i$. We shall show that these are the numbers satisfying the requirements of the theorem.

To this end let n be any integer $> N$ and let C^s be any s-dimensional δ-cycle in A_n of diameter $< d'$. Again as in Lemmas 2. 1 and 2. 3, it is clear that C^s has a Vietoris cycle realization $Z = (z_1, z_2, \cdots)$ in A_n of diameter $d' + 2(d - d')/2 = d$. Also as before $C^s \underset{\delta_s}{\sim} z_k$ in a subset of A_n of diameter $< d + 2\delta_r$ for each k. Whence $C^s \underset{\epsilon}{\sim} z_k$ for all k since $\delta_r \leqq \epsilon$.

Now since $\delta(Z) < d$ and since $n > N$, it follows by hypothesis that $Z \sim 0$ in a subset of A_n of diameter $\leqq e$. The use of the prism construction in the δ_s-homology between C^s and z_k uses no new vertices; hence every point of the complex bounded by $C^s + z_k$ is within a distance δ_s of some point of z_k. Also every point of the ϵ-complex bounded by z_k is within a distance e of any point in z_k; therefore the sum of these two complexes is an ϵ-complex bounded by C^s with diameter $< e + \delta_s < e + \eta$. That is, $C^s \underset{\epsilon}{\sim} 0$ in a subset of A_n of diameter $< e + \eta$, which was to be proved.

We now proceed to the proof of the theorem. To this end consider a sequence $[a_i]$ in $A^s{}_{\bar{e},d}$ converging to a. This implies that $[A_i] \underset{\leqq r}{\rightarrow} A$, and that any γ^s in A_i with diameter $< d$ is homologous to 0 in a subset of A_i of diameter $\leqq e$. If $\eta > 0$ and d' are numbers with $0 < d' < d$, then by Lemma 4. 4 $e + \eta$ and d' are numbers such that for any $\epsilon > 0$ there exist numbers $\delta > 0$ and N such that if $n > N$ and C^s is a δ-cycle in A_n of diameter $< d'$ then $C^s \underset{\epsilon}{\sim} 0$ in a subset of A_n of diameter $< e + \eta$ and hence $\leqq e + \eta$. Now by Lemma 4. 3, any complete s-dimensional cycle in A of diameter $< d'$ is ~ 0 in a subset of A of diameter $\leqq e + \eta$. Since d' and η are arbitrary, we can conclude that every complete cycle in A of diameter $< d$ is ~ 0 in a subset of A of diameter $< e + \eta$ for all $\eta > 0$. Thus if $[\eta_j]$ is a sequence converging to 0, then there exist complexes $[D_j{}^{s+1}]$ such that $\dot{D}_j{}^{s+1} = C^s$ and $\delta(D_j{}^{s+1}) < e + \eta_j$ where $D_j{}^{s+1} \subset A$. We can suppose the η_j's so chosen that the point sets $[D_j{}^{s+1}]$ converge to a limit L. Clearly $\delta(L) \leqq e$ and L contains the point set C^s. We shall exhibit a complete $(s+1)$-chain in L bounded by C^s. To this end consider a strictly monotone decreasing sequence $[\alpha_j] \rightarrow 0$. We can pick a subsequence of the point sets $[D_j{}^{s+1}]$, suppose it to be the whole sequence, such that $U_{\alpha_j/3}(D_j{}^{s+1})$ contains L and $U_{\alpha_j/3}(L)$ contains $D_j{}^{s+1}$ for each j.

Corresponding to $\alpha_j/3$ there is a number N_j such that if $D_j^{s+1} = (D_{1j}^{s+1}, D_{2j}^{s+1}, \cdots)$, then for $i > N_j$, D_{ij}^{s+1} is an $\alpha_j/3$-complex. Project each of the D_{ij}^{s+1} for $i > N_j$ by means of an $\alpha_j/3$ projection [12] into a complex E_{ij}^{s+1} of L keeping points of C_i^s fixed. Clearly, for $i > N_j$, $\delta(E_{ij}^{s+1}) \leqq e$ and E_{ij}^{s+1} is an α_j-complex for all i such that $\dot{E}_{ij}^{s+1} = C_i^s$. We do this for each j and define a complete complex E^{s+1} as follows:

$$E^{s+1} = (E^{s+1}_{1,1}, E^{s+1}_{2,1}, \cdots, E^{s+1}_{N_1,1}, E^{s+1}_{N_1+1,1}, E^{s+1}_{N_1+2,1}, \cdots, E^{s+1}_{N_1+N_2-1,1}, \\ E^{s+1}_{N_1+N_2,2}, E^{s+1}_{N_1+N_2+1,2}, \cdots, E^{s+1}_{N_1+N_2+N_3,3}, \cdots, E^{s+1}_{N_1+N_2+\cdots+N_j,j}, \cdots)$$

Now $\dot{E}_{ij_i}{}^{s+1} = C_i^s$ for each i and $\delta(E_{ij_i}{}^{s+1}) \leqq e$. Finally consider any number $\alpha > 0$; there exists an $\alpha_n < \alpha$ and any $i > N_1 + N_2 + \cdots + N_n$. This implies that $E_{ij_i}{}^{s+1}$ is an α-complex; hence $C^s \underset{\alpha}{\sim} 0$ for all $\alpha > 0$, or $C^s \sim 0$ in a subset of A of diameter $\leqq e$. This tells us that $a \in K^s{}_{\bar{e},d}$ which is therefore closed.

COROLLARY 4.21. *$K_{\bar{e},d}$ is closed for each $e > 0$ and $d > 0$.*

Proof. By definition $K_{\bar{e},d} = \prod_{s \leqq r} K^s{}_{\bar{e},d}$, where $K^s{}_{\bar{e},d}$ is closed by Theorem 4.2. Now $K_{\bar{e},d}$ is closed for, by Theorem 3.7, K is a Hausdorff space in which it is always true that the product of any number of closed sets is closed.

COROLLARY 4.22. $\prod_{\eta > 0} K^s{}_{e+\eta,d} = K^s{}_{\bar{e},d}$.

Proof. This follows immediately from a part of the proof. That is, we showed that if every complete cycle in A of diameter $< d$ is ~ 0 in a subset of A of diameter $< e + \eta$ for all $\eta > 0$, then every complete cycle of diameter $< d$ bounds in a subset of diameter $\leqq e$, or in other words $\prod_{\eta > 0} K^s{}_{e+\eta,d} \subset K^s{}_{\bar{e},d}$. The inclusion in the other direction follows immediately from the definitions of the sets involved, hence the equality.

COROLLARY 4.23. $\prod_{\eta > 0} K_{e+\eta,d} = K_{\bar{e},d}$.

Proof. $K_{e+\eta,d} = \prod_{s \leqq r} K^s{}_{e+\eta,d}$; $\prod_{\eta > 0} K_{e+\eta,d} = \prod_{\eta > 0} \prod_{s \leqq r} K^s{}_{e+\eta,d} = \prod_{s \leqq r} \prod_{\eta > 0} K^s{}_{e+\eta,d}$
$$= \prod_{s \leqq r} K^s{}_{\bar{e},d} = K_{\bar{e},d}.$$

THEOREM 4.5. *$K^s{}_{e-\sigma,\bar{d}}$ is interior to $K^s{}_{\bar{e},d}$.*

Proof. Suppose that the theorem were false; then there would be a point p in $K^s{}_{e-\sigma,\bar{d}}$, but not interior to $K^s{}_{\bar{e},d}$. That is, there exists a sequence $[p_i]$ of

---

[12] See footnote [6].

points in $C(K^s{}_{\bar{e},d})$ converging to p, or $[P_i] \underset{\leqq r}{\rightarrow} P$, where each P_i is lc^r. Now $e - \sigma$ and d are numbers such that every γ^s of P with diameter $\leqq d$ is homologous to 0 in a subset of P of diameter $< e - \sigma$ by the definition of $K^s{}_{e-\sigma,\bar{d}}$. But by Lemma 2. 3 where $\epsilon = e - \sigma$, $s = r$, $\delta_s = d$, and $\sigma = \sigma$ we know that there exists a number N such that if $i > N$, then every γ^s in P_i with diameter $\leqq d$ is homologous to 0 in a subset of P of diameter $< e - \sigma + \sigma = e$. This says that for $i > N$ $p_i \epsilon K^s{}_{e,\bar{d}} \subset K^s{}_{\bar{e},d}$ which is contrary to our hypothesis; hence the theorem is true.

Corollary 4. 51. *$K_{e-\sigma,\bar{d}}$ is interior to $K_{\bar{e},d}$.*

Proof. $K_{e-\sigma,\bar{d}} = \prod_{s \leqq r} K^s{}_{e-\sigma,\bar{d}} \subset \prod_{s \leqq r}$ (interior of $K^s{}_{\bar{e},d}$) by Theorem 4. 5. This in turn is contained in the interior of $\prod_{s \leqq r} K^s{}_{\bar{e},d}$, since K is a Hausdorff space, but this latter set is the interior of $K_{\bar{e},d}$ which was to be proved.

Theorem 4. 6. *K is regular.*

Proof. Let O_p be any open set containing a point p. Consider a strictly monotone decreasing sequence $[e_i] \rightarrow 0$. Since P is lc^r, for each e_i there is a $d_i < e_i$ such that if γ^s is a complete cycle in P with diameter $\leqq d_i$ where s is any number $\leqq r$, then $\gamma^s \sim 0$ in a subset of P of diameter $< e_i/2$. Thus for all i, $p \epsilon K_{e_i-(e_i/2),d_i} \subset K_{\bar{e}_i,d_i}$. Let $A_n = \prod_1^n K_{\bar{e}_i,d_i} \cdot \bar{A}_{e_n,p}$. By Corollary 4. 21 each $K_{\bar{e}_i,d_i}$ is closed. Now there exists an N such that $A_n \subset O_p$; for if not, then there exists a point p_n in the set $A_n \cdot C(O_p)$ for each n. Since $e_{n-1} > e_n$, we have $\bar{A}_{e_n,p} \subset A_{e_{n-1},p}$ for each n; hence $[P_n] \rightarrow P$. Also for any $e > 0$ there is an $e_m < e$, and we shall let $d = d_m$. Now consider P_k for $k \geqq m$, and a γ^s in P_k for some $s \leqq r$ such that $\delta(\gamma^s) < d$. Since $k \geqq m$, $p_k \epsilon K_{\bar{e}_i,d_i} \subset K_{\bar{e}_m,d_m}$ and $\gamma^s \sim 0$ in a subset of A_k of diameter $\leqq e_m < e$. This says that $[P_n] \underset{\leqq r}{\rightarrow} P$ or $[p_n] \rightarrow p$, but this is impossible as each p_n was in $C(O_p)$ which is closed. Now by Corollary 4. 51 $p \epsilon K_{e_i-e_i/2,\bar{d}_i} \subset$ interior of $K_{\bar{e}_i,d_i}$ for all i. It follows that $p \epsilon \prod_1^N K_{e_i-(e_i/2),\bar{d}_i} \cdot A_{e_N,p} \subset \prod_1^N$ interior $K_{\bar{e}_i,d_i} \cdot A_{e_N,p} \subset$ interior $\prod_1^N K_{\bar{e}_i,d_i} \cdot A_{e_N,p} \subset \prod_1^N K_{\bar{e}_i,d_i} \cdot A_{\bar{e}_N p} = A_N \subset O_p$. If we let $U_p = \prod_1^N$ interior $K_{e_i,d_i} \cdot A_{e_N,p}$ which is open, then $\bar{U}_p \subset \bar{A}_N = A_N \subset O_p$ and K is regular.

Corollary 4. 61. *Corresponding to any point p, there exists a countable monotone decreasing sequence of open sets $[O_i]$ whose product is p, and such that if U is any open set containing p, then there is a number N such that $O_N \subset U$.*

Proof. Let $O_k = \prod_1^k \text{interior } K_{\bar{e}_i, d_i} \cdot A_{e_k, p}$ as in the proof of Theorem 4. 6. Then $\prod_1^\infty O_i = p$ for if not there exists a point q different from p in $\prod_1^\infty O_i$. But by Theorem 3. 6 there exists an open set U_p containing p such that $q \notin U_p$ and by the proof of Theorem 4. 6 there exists a number N such that $\bar{O}_N \subset U_p$. Thus $\prod_1^\infty O_i \subset O_N \subset \bar{O}_N \subset U_p$, contrary to the assumption that q is in $\prod_1^\infty O_i \cdot C(U_p)$.

Also in the proof of Theorem 4. 6 the second half of the theorem is proved.

5. The metrization and separability of *K*.

THEOREM 5. 1. *Corresponding to any set* $R_{\bar{\epsilon}, \delta} = \sum_{\eta > 0} K_{\overline{\epsilon - \eta}, \delta + \eta}$ *there is a continuous function f of K into the interval* $0 \leqq x \leqq \epsilon$ *such that* $f(R_{\bar{\epsilon}, \delta}) > 0$ *and* $f(C(R_{\bar{\epsilon}, \delta})) = 0$.

Proof. We define $f(p)$ as follows: If $p \in R_{\bar{\epsilon}, \delta}$, $f(p) = \text{l. u. b. } \eta$ such that $p \in K_{\overline{\epsilon - \eta}, \delta + \eta}$. If $p \notin R_{\bar{\epsilon}, \delta}$, $f(p) = 0$. Clearly $0 \leqq f(p) \leqq \epsilon$. Now f is continuous, for consider $[p_i] \to p$. Let η_1 be any number $> f(p)$; then by definition of $f(p)$ we have $p \notin K_{\overline{\epsilon - \eta_1}, \delta + \eta_1}$. By Corollary 4. 21, $K_{\overline{\epsilon - \eta_1}, \delta + \eta_1}$ is closed and hence $C(K_{\overline{\epsilon - \eta_1}, \delta + \eta_1})$, which contains p, is open. This implies that almost all $[p_i]$ are in $C(K_{\overline{\epsilon - \eta_1}, \delta + \eta_1})$ and hence $f(p_i) \leqq \eta$, for almost all i. This completes the proof of the continuity if $p \in C(R_{\bar{\epsilon}, \delta})$. If, however, $p \in R_{\bar{\epsilon}, \delta}$, let $\eta_2 > 0$ be any number $< f(p)$ and pick η_3 such that $\eta_2 < \eta_3 < f(p)$. Now $p \in K_{\overline{\epsilon - \eta_3}, \delta + \eta_3}$ by the definition of $f(p)$. We can now show that almost all $[p_i] \subset K_{\overline{\epsilon - \eta_2}, \delta + \eta_2}$. To this end let $2\sigma = \eta_3 - \eta_2$. Now $\eta_2 < \eta_3$ and $\delta + \eta_2 < \delta + \eta_3$, $\epsilon - \eta_3 < \epsilon - (\eta_3 - \sigma)$, $p \in K_{\overline{\epsilon - \eta_3}, \delta + \eta_3} \subset K_{\epsilon - (\eta_3 - \sigma), \overline{\delta + \eta_2}}$. By Lemma 2.3 almost all $[p_i] \subset K_{\epsilon - (\eta_3 - \sigma) + \sigma, \overline{\delta + \eta_2}} = K_{\epsilon - (\eta_3 - 2\sigma), \overline{\delta + \eta_2}} = K_{\epsilon - \eta_2, \overline{\delta + \eta_2}} \subset K_{\overline{\epsilon - \eta_2}, \delta + \eta_2}$, therefore $f(p) \geqq \eta_2$ for almost all i. Now $\eta_2 < f(p) < \eta_1$ where η_2 and η_1 were arbitrary and we have just shown that for almost all i $\eta_2 \leqq f(p_i) \leqq \eta_1$; hence $[f(p_i)]$ converges to $f(p)$ which concludes the continuity proof.

Furthermore if $p \in C(R_{\bar{\epsilon}, \delta})$, $f(p) = 0$ by definition. Finally if $p \in R_{\bar{\epsilon}, \delta}$, then $p \in K_{\overline{\epsilon - \eta}, \delta + \eta}$ for some $\eta > 0$ and $f(p) \geqq \eta > 0$. This concludes the proof of the theorem.

THEOREM 5. 2. *H (and hence K) is a subset of Hilbert space if we understand that ordinary convergence takes the place of regular convergence in the definition of a limit point (that is, $[p_i] \to p$ if and only if $[P_i] \to P$).*

Proof. Although this theorem is by no means new, its proof follows almost immediately from our previous work. We have only to note that in most of our theorems it was necessary to prove convergence first and then regular convergence. Thus if we leave off the part of our proofs about regular convergence, we get the same theorems for H with this new limit notion, that we proved before for K. In fact we can say that H is a regular Hausdorff space, for each of the theorems involved in proving this are of the character described above. It remains to show the existence of a fundamental sequence of regions in H. To do this we note that since M is compact and metric, it has a fundamental sequence of regions $(R_1, R_2, \cdots)$. Define $p_{i_1 i_2 \ldots i_n}$ to be the point of H corresponding to $\overline{R_{i_1} + R_{i_2} + \cdots + R_{i_n}}$; then the collection $[p_{i_1 \ldots i_n}]$, where n and each i_j range over all integers will be shown to be everywhere dense in H. If p is a point of H then P is compact and can be covered by a monotone decreasing sequence of sets $R_{i_{11}} + R_{i_{12}} + \cdots + R_{i_{1n_1}} \supset R_{i_{21}} + R_{i_{22}} + \cdots + R_{i_{2n_2}} \supset \cdots$ whose product is P. Thus the sequence $[p_{i_{j1}, i_{j2}, \ldots i_{jn_j}}] \to p$ as $j \to \infty$. Now we can associate with each $p_{i_1 i_2 \ldots i_n}$ the sequence $[A_{1/k, p_{i_1 i_2 \ldots i_n}}]$. This gives a countable collection of sets which serve as a fundamental sequence. For consider a point p and any open set U containing p. There will be a set $A_{1/2k,p} \subset U$ and a point $p_{i_1 i_2 \ldots i_n} \in A_{1/2k,p}$. Now $A_{1/2k, p_{i_1 \ldots i_n}}$ contains p and $\in A_{1/k,p} \subset U$, which is the defining property of a fundamental sequence. It is a well known result that we can set up the Hilbert metric in such a space, and since K is a subset of H, it too is homeomorphic with a subset of the Hilbert space.

THEOREM 5. 3. *K can be metrized by means of the Hilbert metric in such a way that the regular convergence definition of a limit point is preserved.*

Proof. Let us consider the sequence $[1/2^{i/2}]$, and let $\delta_i = \epsilon_i = 1/2^{i/2}$, $(i = 1, 2, \cdots)$. In Theorem 5. 1 denote by f_{ij} the function corresponding to $R_{\epsilon_i, \delta_j}^{-}$. Finally let $f_{0j}(p) = 2^{j/2}$ (the j-th coördinate of p in the Hilbert metric established in Theorem 5. 2). Then the distance under this metric between two points p and q of K would be $\rho_1(p, q) = \sqrt{\sum_{j=1}^{\infty} \frac{(f_{0j}(p) - f_{0j}(q))^2}{2^j}}$, where $\sum_{j=1}^{\infty} f_{0j}^2(p)/2^j$ exists for all p in K.

The Hilbert coördinates of this theorem will be $[f_{ij}(p)/2^{j/2}]$ where $(0 \leqq i < j)$, $(j = 1, \cdots)$, and we shall define $\rho(p, q) = \sqrt{\sum_{j=1}^{\infty} \sum_{i=0}^{j} \frac{(f_{ij}(p) - f_{ij}(q))^2}{2^j}}$.

We may think of the coördinates as a single sequence where $f_{ij}(p)/2^{j/2}$

precedes $f_{kl}(p)/2^{l/2}$ if $j < l$, or if $j = l$ and $i < k$. These are possible Hilbert coördinates for $\sum_{j=1}^{\infty} \sum_{i=0}^{j} \frac{f_{ij}^2(p)}{2^j} = \sum_{j=1}^{\infty} \sum_{i=1}^{j} \frac{f_{ij}^2(p)}{2^j} + \sum_{j=1}^{\infty} \frac{f_{0j}^2(p)}{2^j}$. We already know that the second part converges so we need only consider the first. We recall that $f_{ij}(p) \leqq \epsilon_i$; hence $\sum_{i=1}^{\infty} \sum_{i=1}^{j} \frac{f_{ij}^2(p)}{2^j} \leqq \sum_{j=1}^{\infty} \sum_{i=0}^{j} \frac{\epsilon_i^2}{2^j} < \sum_{j=1}^{\infty} \frac{1}{2^j} = 1$. Thus both the first and second, and hence the entire series converges.

We now proceed to prove that $\rho(p, q)$ has the several properties of a metric. For simplicity let $\rho_2(p, q) = \sqrt{\sum_{j=1}^{\infty} \sum_{i=1}^{j} \frac{(f_{ij}(p) - f_{ij}(q))^2}{2^j}}$

1) That $\rho(p, q)$ is defined and $\geqq 0$ for all p and q follows from the above discussion and the fact that all terms are positive.

2) Clearly $\rho(p, q) = \rho(q, p)$.

3) $\rho(p, q) = 0$ if and only if $p = q$.
Clearly $\rho(p, q) = 0$ if $p = q$. Conversely, if $\rho(p, q) = 0$ then $f_{0j}(p) = f_{0j}(q)$ for all j, hence $\rho_1(p, q) = 0$ and $p = q$ since ρ_1 is a metric.

4) The triangle inequality follows in the usual way for this type of metric.

5) The point p is a limit point of the set E if and only if for any $\epsilon > 0$, there exists a point q of E such that $\rho(p, q) < \epsilon$.

First let p be a limit point of a set E, then there exists a sequence of distinct points $[p_k]$ of E converging to p. This means that $[P_k] \underset{\leqq r}{\rightarrow} P$. Since $[P_k] \rightarrow P$, there exists a number N_1 such that for $k > N_1$ $\rho_1(p, p_k) < \epsilon/2$. Also there is a number N_2 such that $\sum_{j=N_2+1}^{\infty} 1/2^j < \epsilon/4$. Let $\sum_{j=1}^{N_2} \sum_{i=1}^{j} 1/2^j = K$. By the continuity of f_{ij} $(i \neq 0)$ we can find an N_3 such that for $k > N_3$, $|f_{ij}(p) - f_{ij}(p_k)| < \epsilon/4K$ $(i = 1, \cdots, j;\ j = 1, \cdots, N_2)$. Thus for $k > N_2 + N_3$, $\rho_2(p, p_k) < \epsilon/4K \cdot (\sum_{j=1}^{N_2} \sum_{i=1}^{j} i/2^j) + \epsilon/4 < \epsilon/4K \cdot K + \epsilon/4 < \epsilon/4 + \epsilon/4 = \epsilon/2$. Finally $\rho(p, p_k) \leqq \rho_1(p, p_k) + \rho_2(p, p_k)$. Therefore for $k > N_1 + N_2 + N_3$, $\rho(p, p_k) < \epsilon/2 + \epsilon/2 = \epsilon$.

Conversely, suppose that for each $\epsilon > 0$ there is a point q in E different from p such that $\rho(p, q) < \epsilon$, but that p is not a limit point of E. This implies that $p \notin E'$ and hence not in $\bar{E} - p$ which is closed. Thus $p \in C(\bar{E} - p)$ which is open. Now for each ϵ_{i+1} there exists a number $\delta < \epsilon_{i+1}$ by virtue of the local γ^s-connectedness of P for $s \leqq r$ such that $p \in K_{\bar{\epsilon}_{i+1}, \delta}$. Let $\eta = (\sqrt{2} - 1)\delta$ and $\epsilon' = \epsilon_{i+1} + \eta < \sqrt{2}\,\epsilon_{i+1} = \epsilon_i$, $\delta' = \delta - \eta$. Then p is in $K_{\overline{\epsilon' - \eta}, \delta' + \eta}$. Finally let δ_{j_i} be any member of our original sequence $[\delta_i]$ such that $\delta_{j_i} < \delta'$. Clearly we also have $p \in K_{\overline{\epsilon_i - \eta}, \delta_{j_i} + \eta} \subset R_{\bar{\epsilon}_i, \delta_{j_i}}$. Also it follows readily from the definitions

that $R_{\bar{\epsilon}_i,\delta_{j_i}} \subset K_{\bar{\epsilon}_i,\delta_{j_i}}$. Now in proving Theorem 4.6 we showed that corresponding to any open set and a point in it there is a number N such that p is in $\prod_{i=1}^{N} (R_{\bar{\epsilon}_i,\delta_{j_i}}) \cdot \bar{A}_{p,\delta_{jN}} \subset \prod_{i=1}^{N} K_{\bar{\epsilon}_i,\delta_{j_i}} \cdot \bar{A}_{p,\delta_{jN}} \subset [C(\bar{E} - p)]$. The definition of $A_{p,\delta_{jN}}$ has already been given (Definition 4.1), but if we think of it here as the set of points q such that $\rho(q,p) < \delta_{jN}$, it is clear that the proof follows just as before. Now by Theorem 5.1 $f_{ij_i}(p) > 0$ for $i = 1, \cdots, N$ since $p \in R_{\bar{\epsilon}_i,\delta_{j_i}}$; hence we can let $L =$ the smallest of the numbers $f_{ij_i}(p)$ for $i = 1, \cdots, N$. By hypothesis there exists a point q different from p and ϵE such that $\rho(p,q) < \min. (\delta_{jN}, L \cdot \delta_{jN})$. Since $\rho_1(p,q) \leqq \rho(p,q) < \delta_{jN}$, we have $q \in A_{p,\delta_{jN}}$ where we use the modified definition of this set. Also $|f_{ij}(p) - f_{ij}(q)|/2^{j/2} = \sqrt{\dfrac{(f_{ij}(p) - f_{ij}(q))^2}{2^j}} \leqq \rho_2(p,q) \leqq \rho(p,q) < L \cdot \delta_{jN}$ for any $i = 1, \cdots, N$. Hence $|f_{ij}(p) - f_{ij}(q)| < L \cdot (\delta_{jN}/\delta_{j_i}) < L$ and $f_{ij_i}(q) > f_{ij_i}(p) - L \geqq 0$ for $i = 1, \cdots, N$. By Theorem 5.1 this implies that $q \in R_{\bar{\epsilon}_i,\delta_{j_i}}$ for $i = 1, \cdots, N$, and $q \in \prod_{i=1}^{N} R_{\bar{\epsilon}_i,\delta_{j_i}} \cdot \bar{A}_{p,\delta_{jN}} \subset \prod_{i=1}^{N} K_{\bar{\epsilon}_i,\delta_{j_i}} \cdot \bar{A}_{p,\delta_{jN}} \subset C(\bar{E} - p)$. This however contradicts the fact that $q \neq p$ and $q \in E$, and p must be a limit point of E. This concludes the proof of the theorem.

COROLLARY 5.31. *K is separable.*

Proof. This follows since, by Theorem 5.3, K (with the regular convergence limit notion) is homeomorphic with a subset of Hilbert space which is separable.

COROLLARY 5.32. *Contained in any compact metric space M is a countable collection of closed locally connected subsets such that a subsequence of the collection can be found corresponding to any closed locally connected subset of M which converges to it 0-regularly. Furthermore if M is locally connected then a subsequence can be found corresponding to any closed subset of M which converges to it in the ordinary sense.*

Proof. The first part is merely a restatement of Corollary 5.31 where $r = 0$, for local γ^0-connectedness is exactly the same as local connectedness in compact spaces. The second part is also immediate for if M is locally connected then the locally connected closed subsets are everywhere dense in the space of all closed subsets where the ordinary convergence notion is used. Thus if our collection has subsequences converging regularly to all closed locally connected subsets, it also has subsequences converging to any closed subset.

6. The connectivity of K. A large part of this section is dependent on some general theorems on Betti numbers which are now stated.

THEOREM 6.1. *The r-dimensional Betti number $p^r(M)$ of M is finite if M is lc^r.*

Proof. This is a theorem of R. L. Wilder. For the proof see the *Duke Mathematical Journal*, vol. 1 (1935), p. 546.

THEOREM 6.2. *If the sequence of closed sets $[A_i] \underset{\leqq r}{\rightarrow} A$, and $p^s(A) = n$ for some $s \leqq r$, then there exists a number N such that for $i > N$ $p^s(A_i) \geqq n$.*

THEOREM 6.3. *If the sequence of closed sets $[A_i] \underset{\geqq r}{\rightarrow} A$, and for some number $s \leqq r$ $p^s(A) = n$, then there exists an N such that for $i > N$ $p^s(A_i) \leqq n$.*

Both of the above two theorems are due to H. A. Arnold, but have not as yet been published. The following three corollaries follow immediately from these theorems.

COROLLAR 6.31. *If the sequence of closed sets $[A_i] \underset{\leqq r}{\rightarrow} A$ where $p^s(A) = n$ for some number $s \leqq r$, then there exists a number N such that for $i > N$ $p^s(A_i) = n$.*

COROLLARY 6.32. *If the sequence of closed sets $[A_i] \underset{\leqq r}{\rightarrow} A$ where for almost all i $p^s(A_i) = n$ for a number $s \leqq r$, then $p^s(A) = n$.*

COROLLARY 6.33. *If the sequence of closed sets $[A_i] \underset{\leqq r}{\rightarrow} A$ where for almost all i $p^s(A_i) \neq n$ for a number $s \leqq r$, then $p^s(A) \neq n$.*

DEFINITION 6.1. We shall denote by $K_{n_0, n_1, \ldots, n_r}$ the set of all points p of K corresponding to subsets P of M such that $p^s(P) = n_s$ $(s = 0, \cdots, r)$.

THEOREM 6.4. *$K_{n_0, n_1, \ldots, n_r}$ is both open and closed for all numbers $n_s \geqq 0$, $0 \leqq s \leqq r$.*

Proof. If p is a limit point of the set in question, then there exists a sequence $[p_i]$ of points in $K_{n_0, n_1, \ldots, n_r}$ such that $[p_i] \rightarrow p$. This means that $p^s(P_i) = n_s$ for all i which implies by corollary 6.32 that $p^s(P) = n_s$ for each $s \leqq r$, hence $p \in K_{n_0, n_1, \ldots, n_r}$. This proves the set is closed.

Next we show the set is open for if it were not then a point p of it would exist together with a sequence $[p_i]$ of the complement converging to it. That is $[P_i] \underset{\leqq r}{\rightarrow} P$ where $p^s(P) = n_s$ for $s \leqq r$. But by Corollary 6.31 $p^s(P_i) = n_s$ for almost all i and each $s \leqq r$; hence $p_i \in K_{n_0, n_1, \ldots, n_r}$ for almost all i, contradicting the hypotheses on them. Thus $K_{n_0, n_1, \ldots, n_r}$ must also be open.

DEFINITION 6.2. Let $K_{n_s}{}^s = \sum_{n_i=0,\, i\neq s}^{\infty} K_{n_0, n_1, \ldots, n_s, \ldots, n_r}$.

THEOREM 6.5. *The set $K_{n_s}{}^s$ is both open and closed for all numbers $s \leqq r$ and $n_s \geqq 0$.*

Proof. The proof is the same as that of Theorem 6.4 if we fix our attention on a particular s throughout the discussion.

COROLLARY 6.51. *K will be connected if and only if M is a single point.*

Proof. If K is connected, then $K = K_1{}^0$.[13] Thus M cannot contain two points and $M =$ a single point.

Conversely if $M =$ a single point, it is clear that K is a single point which is connected.

COROLLARY 6.52. *K will have a finite number of components if and only if M is finite.*

Proof. If K has only a finite number of components, then since $K = \sum_{i=0}^{\infty} K_i{}^0$, we have $K_i{}^0 = 0$ for all $i >$ some number N. That is, there exists no locally γ^s-connected subset with more than N components. In particular, M cannot contain more than N points.

Conversely, it is clear that if M is finite then so is K, and K has only a finite number of components.

THEOREM 6.6. *If $M = M_1 + M_2 + \cdots + M_n$, where M_i is open and closed for each i, then $K_1{}^0 = K_{1,1}{}^0 + K_{1,2}{}^0 + \cdots + K_{1,n}{}^0$ where each $K_{1,i}{}^0$ is both open and closed.*

Proof. Define $K_{1,i}{}^0 = K_1{}^0 \cdot h_K(M_i)$, $i = 1, \cdots, n$. By Theorem 6.5 $K_1{}^0$ is both open and closed. By Theorem 3.4 and 3.5 $h_K(M_i)$ is both open and closed, and hence so is the product $K_{1,i}{}^0$. Now $K_1{}^0 \subset \sum_{i=1}^{n} K_{1,i}{}^0$, for if $p \in K_1{}^0$, then P is a locally γ^s-connected continuum and is contained in one set M_i. That is, $p \in h_K(M_i) \cdot K_1{}^0 = K_{1,i}{}^0$ and $K_1{}^0 \subset \sum_{i=1}^{n} K_{1i}{}^0$. Now clearly $\sum_{i=1}^{n} K_1{}^0 \cdot \subset K_{1i}{}^0$ and $K_1{}^0 = \sum K_{1i}{}^0$ which was to be proved.

---

[13] We assume that a 0-dimensional cycle is any number of points in this discussion. This implies that $p^0(M) =$ the component number.

THEOREM 6.7. *If $K_1{}^0$ is disconnected and has m components, then $K_n{}^0$ is disconnected, and has at least $\sum_{i=1}^{n} {}_mC_i \cdot {}_nS_i$ components where ${}_mC_i$ is the number of combinations of m things i at a time and ${}_nS_i$ is the number of permutations of positive integers whose sum is n taken i at a time with repetitions allowed.*

Proof. By definition every point of $K_n{}^0$ corresponds to a set with n components. Suppose these components to be picked from i of the m components of $K_1{}^0$ and that $j_1, j_2, \cdots, j_i$ are the numbers of components of the set which correspond to the i different components. Thus $j_1 + j_2 + \cdots + j_i = n$. Now clearly the i components can be chosen in ${}_mC_i$ ways and the n components of the set can be picked so that their correspondents in K come from the i components in ${}_nS_i$ ways. Therefore, there are ${}_mC_i \cdot {}_nS_i$ choices in all if i components are used, hence in all $\sum_{i=1}^{m} {}_mC_i \cdot {}_nS_i$ choices. Now consider a subset C of $K_n{}^0$ corresponding to all sets chosen in one of the above ways. Suppose $K_1{}^0 = \sum_{j=1}^{m} K_{1j}$, where $[K_{1j}]$ are the components of $K_1{}^0$. Now each point in C corresponds to a set with J_1 components corresponding to points in K_{1k_1, j_2} components in $K_{1k_2, \ldots, j_i}$ components in K_{1k_i}. C is closed, for consider $[p_i] \subset C$ such that $[p_i] \to p$ or $[P_i] \underset{\leqq r}{\to} P$. Now P has n components since $K_n{}^0$ is closed. Also a subsequence of $[P_i]$ can be picked such that there exist n component sequences converging $\leqq r$-regularly to n components of P and such that each sequence is contained entirely in the same set K_{1q}. Since each K_{1q} is closed, each component of P belongs to the same set K_{1q} as the members of the sequence converging to it and $p \in C$.

An entirely analogous argument shows that $K_n{}^0 - C$ is closed which implies C is open as well as closed in $K_n{}^0$. Thus each component of $K_n{}^0 \subset$ one of the sets C which implies that the number of components is $\geqq$ (number of sets C) $= \sum_{i=1}^{m} {}_mC_i \cdot {}_nS_i$.

Theorem 6.7 leads us to restrict our connectivity considerations to the set $K_1{}^0$.

DEFINITION 6.3. We shall say that a subset P of M can be $\leqq$ *r-regularly deformed* into a set Q provided there exists a family of set functions $[f_t(P)]$ $(0 \leqq t \leqq 1)$ such that $f_0(P) = P$, $f_1(P) = Q$, $f_t(P) \subset M$ for all t, and if $[t_i] \to t$ then $[f_{t_i}(P)] \underset{\leqq r}{\to} f_t(P)$.

THEOREM 6.8. *A necessary and sufficient condition that the closed lc^r*

subset P of M be $\leqq$ r-regularly deformable into Q is that p and q can be joined by an arc in K.

Proof. Suppose that P can be regularly deformed into Q by means of the set functions $[f_t(P)]$. Then $\sum_{t=0}^{1} f_t(p) \subset K$, where $f_t(p)$ is the point of K corresponding to $f_t(P)$, is a continuous image of the interval $(0 \leqq t \leqq 1)$, and hence a locally connected continuum. Thus it contains an arc from p to q.

Conversely, suppose there exists an arc pq which we shall think of as the homeomorphic image of the interval $(0 \leqq t \leqq 1)$ where 0 corresponds to p and 1 to q. Define $f_t(P)$ to be the set corresponding to the point of the arc associated with t. Clearly this set of functions defines the regular deformability.

COROLLARY 6. 81. *A necessary and sufficient condition that each lc^r subset of M with n components be $\leqq$ r-regularly deformable into any other set of the same type is that $K_n{}^0$ be arcwise connected.*

THEOREM 6. 9. *If M is a continuum containing no simple closed curve then $K_1{}^0$ is connected.*

Proof. Every lc^r subcontinuum is of course locally connected and since it contains no simple closed curve by hypothesis, it must be a dendrite. Now any dendrite D of M can clearly be deformed to any point P of it without going outside of itself, if we remove the regular convergence restriction. That is, there exists a family of set functions $[f_t(D)]$ such that $f_t(D) \subset D$ $(0 \leqq t \leqq 1)$, $f_0(D) = 0$, $f_1(D) = 1$, and $[t_i] \to \bar{t}$ implies $[f_{t_i}(D)] \to f_{\bar{t}}(D)$. But $f_t(D)$ must also be a dendrite for each t and all of the convergence takes place in a dendrite, hence it is easy to see that the convergence is automatically regular. Now by Theorem 6. 8 there exists an arc dp in K and hence in $K_1{}^0$. But the set G of $K_1{}^0$ corresponding to the points of M is clearly connected since M is, hence $K_1{}^0 = G + \sum$ arcs dp is connected.

THEOREM 6. 10. *If $r > 0$ and $K_1{}^0$ is connected, then M is a continuum containing no simple closed curve.*

Proof. By Theorem 6. 6 M is a continuum. Also by Theorem 6. 5 $K_1{}^0$ and $K_0{}^1$ are both open and closed subsets of K. Thus $K_1{}^0 \cdot K_0{}^1$ is both open and closed. But $K_1{}^0$ is connected, hence $K_1{}^0 = K_1{}^0 \cdot K_0{}^1$ or $K_1{}^0 \cdot K_0{}^1 = 0$. Now if $K_1{}^0 = K_1{}^0 \cdot K_0{}^1$ then $K_1{}^0 \subset K_0{}^1$ which implies that M must not contain a simple closed curve, for a simple closed curve would correspond to a point in $K_1{}^0$ but not in $K_0{}^1$. Now $K_1{}^0 \cdot K_0{}^1 = 0$ cannot occur as a single point corresponds to a point in both $K_1{}^0$ and $K_0{}^1$, thus the theorem is true.

The following corollary follows immediately from Theorems 6. 9 and 6. 10.

COROLLARY 6. 10. 1. *If $r > 0$ and M is locally connected, then a necessary and sufficient condition that M be a dendrite is that K_1^0 be connected.*

7. Compactness and local compactness of K.

THEOREM 7. 1. *The properties that K be compact, M be finite, and $H = K$ are equivalent.*

Proof. Suppose that K is compact but that M is infinite. Then there exists a sequence $[p_i]$ of distinct points of M converging to p such that $p_i \neq p$ for any i. Let $Q_i = p_i + p$ for each i. Then $[q_i] \subset K$ is an infinite subset of K with no limit point for although the sets Q_i converge they do not converge 0-regularly nor does any subsequence. Hence M is finite.

Next suppose M is finite; then clearly every subset of M is finite, and hence lc^r. That is, $H = K$.

Finally if $H = K$ but K is not compact, then K must be infinite. This of course implies M is infinite, and we can again find an infinite sequence $[p_i]$ of distinct points of M converging to a point p. But the closed set $[(p_i) + p]$ is not locally γ^0-connected, and thus corresponds to a point of H which is not in K. This contradicts our hypothesis and implies that K is compact.

THEOREM 7. 2. *If $n > 1$, $K_{n,0,0,\ldots,0}$ will be compact if and only if M is finite.*

Proof. If $K_{n,0,0,\ldots,0}$ is compact but M is not finite, then there exists a convergent sequence $[p_i]$ of distinct points of M converging to the point p_0. Now consider the sets $A_i = p_{i+1} + p_{i+2} + \cdots + p_{i+n}$ for $i = 0, 1, 2, \cdots$. Clearly $a_i \in K_{n,0,\ldots,0}$ for all i but the infinite set $\sum_{i=0}^{\infty} a_i$ contains no limit point. This contradicts compactness and M must be finite.

Conversely, if M is finite so is K and the subset $K_{n,0,\ldots,0}$ which is therefore compact.

COROLLARY 7. 21. *If $n > 1$, a necessary and sufficient condition that K_n^0 be compact is that M be finite.*

Proof. If K_n^0 is compact so is its closed subset $K_{n,0,\ldots,0}$ and by Theorem 7. 2 M is finite. The converse is obvious.

THEOREM 7. 3. *A necessary and sufficient condition that K_1^0 be compact is that M contain no non-0-regular convergent sequence of arcs (i. e. every convergent sequence of arcs in M converges 0-regularly).*

Proof. If K_1^0 is compact, then every convergent sequence of locally γ^s-connected ($s \leqq r$) continua in M must converge regularly. For if not we could get by Theorem 1.4 a sequence no subsequence of which converges regularly, and the points of K corresponding to this subsequence would have no limit points. In particular, every convergent sequence of arcs converges regularly and hence 0-regularly.

Conversely, if M has the desired property, then it must contain no simple closed curve. For clearly there exists a non-0-regular convergent sequence of arcs on any simple closed curve. Thus every lc^r continuum of M is a dendrite and contains no complete cycles of dimension $\geqq 1$. Now if K_1^0 were not compact there would be a sequence $[p_i]$ of distinct points in K_1^0 which contains no convergent subsequence. We can suppose that $[P_i]$ converges in the ordinary sense; and since by the above each P_i is a dendrite, this convergence is s-regular for $1 \leqq s \leqq r$. Hence if $[P_i]$ does not converge regularly, it does not converge 0-regularly. This implies that for some $\epsilon > 0$ there exists a sequence of point pairs in the successive sets $P_i \not\subset$ in a continuum of P_i of diameter $< \epsilon$.[14] In particular the arc joining this point pair has diameter $\geqq \epsilon$. Clearly this sequence of arcs does not converge 0-regularly contradicting our hypothesis and we conclude that K_1^0 is compact.

COROLLARY 7.31. *A necessary and sufficient condition that K_1^0 be a continuum is that M be a continuum containing no non-0-regular convergent sequence of arcs.*

Proof. If K_1^0 is a continuum then M is a continuum by Theorem 6.6 and has the desired property by Theorem 7.3. Conversely, if M has the above property then it certainly contains no simple closed curve and by Theorem 6.9 K_1^0 is connected. Finally by Theorem 7.3 K_1^0 is compact, and hence a continuum.

COROLLARY 7.32. *If M is locally connected, then a necessary and sufficient condition that K_1^0 be compact is that every component of M shall be a dendrite.*

Proof. If every component of M is a dendrite, then M contains no non-0-regular convergent sequence of arcs, and by Theorem 7.3 K_1^0 is compact. Conversely, if K_1^0 is compact, then by Theorem 7.3 M contains no non-0-regular convergent sequence of arcs, hence contains no simple closed curve, and hence each component is a dendrite.

---

[14] It is easy to see that if in the definition of 0-regular convergence, we think of a 0-cycle as a pair of points, then ~ 0 means that the pair lie in a continuum.

The next corollary follows in the same way from Corollary 7.31.

COROLLARY 7.33. *If M is locally connected, then a necessary and sufficient condition that K_1^0 be a continuum is that M be a dendrite.*

We now establish a few properties of continua with the property that they contain no non-0-regular convergent sequence of arcs.

THEOREM 7.4. *If M is a continuum containing no non-0-regular convergent sequence of arcs then*

a) *M contains no simple closed curve.*

b) *If M is arc-wise connected it is a dendrite.*

c) *For each point p the set D_p consisting of all points q of M such that there exists an arc pq in M is a dendrite ($D_p =$ the maximal local connected subset of M containing p).*

d) *The sets $[D_p]$ form an upper semi-continuous decomposition of M.*[15]

Proof. a) has been mentioned several times before. b) If M is arc-wise connected, then M is uniformly locally connected. For if not there exists a number ϵ, a sequence $[\delta_i] \to 0$, and a sequence of point pairs (p_i, q_i) such that $\rho(p_i, q_i) < \delta_i$ but $p_i + q_i$ is not contained in a continuum of diameter less than ϵ. In particular, there is an arc p_iq_i with diameter $< \epsilon$. Clearly no subsequence of these arcs converges 0-regularly contrary to hypothesis. Now if M is locally connected, then by Theorems 7.3 and 7.33 we conclude that M is a dendrite. c) D_p is clearly connected. Also D_p is closed; for consider a sequence $[q_i]$ of points of D_p converging to q_0. By definition there exist arcs q_ip_i and we can suppose we have chosen a convergent subsequence. Now by hypothesis $[q_ip_i]$ converges 0-regularly and hence the limit set is an arc[16] containing q_i and p. That is $q_0 \epsilon D_p$ which is thus closed. Now D_p is a continuum with the property that every convergent sequence of arcs converges 0-regularly. Since D_p is clearly arcwise connected, we conclude from b) that D_p is a dendrite. d) It is clear that the sets D_p are disjoint; that is, if $q \epsilon D_p$, then $D_q = D_p$. Also the sets $[D_p]$ cover M and are compact by c). Finally the collection is upper semi-continuous, for consider $[D_{p_i}]$ such that lim. inf. $[D_{p_i}] \cdot D_{p_0} \neq 0$. Let q be contained in lim. sup. $[D_{p_i}]$, then there exists a subsequence $[D_{p_{n_i}}]$ converging to a point set D containing q. Now the convergence must be 0-regular otherwise we could find a non-0-regular convergent

[15] See R. L. Moore, *Transactions of the American Mathematical Society*, vol. 27 (1925), p. 416.

[16] See G. T. Whyburn, "On sequences and limiting sets," *Fundamenta Mathematicae*, vol. 25 (1935), p. 416.

sequence of arcs. Hence D is a dendrite by Corollary 6.32. But D contains p_0 and q; hence $q \epsilon D_{p_0}$ which is sufficient for upper semi-continuity.

THEOREM 7.5. *A necessary and sufficient condition that a compact set M contain no non-0-regular convergent sequence of arcs is that corresponding to every $\epsilon > 0$ there is a $\delta > 0$ such that if p and q are two points of M with $\rho(p, q) < \delta$, then every arc joining p and q has diameter $< \epsilon$.*

Proof. Suppose that M contains no non-0-regular convergent sequence of arcs, but that corresponding to some $\epsilon > 0$ there is a sequence $[\delta_i] \to 0$ and a sequence of point pairs $[p_i, q_i]$ such that $\rho(p_i, q_i) < \delta_i$ but there is an arc $p_i q_i$ of diameter $\geqq \epsilon$ for each i. Clearly this sequence of arcs does not contain a 0-regular convergent subsequence contrary to our hypotheses.

Conversely, suppose that corresponding to each $\epsilon > 0$ there is a $\delta > 0$ with the properties of the theorem. Now consider any convergent sequence of arcs $[a_i b_i]$. If the convergence were not regular, there would be an $\epsilon > 0$ and a sequence of point pairs $p_i + q_i \subset \widehat{a_i b_i}$ such that $\rho(p_i, q_i) < \delta_i$ where $[\delta_i] \to 0$, but such that the subarc $p_i q_i$ has diameter $\geqq \epsilon$. Clearly corresponding to this $\epsilon > 0$ there is no $\delta > 0$ with the properties of the hypothesis; thus the sequence $[a_i b_i]$ must converge 0-regularly.

THEOREM 7.6. *If $K_1{}^0$ is locally compact, then corresponding to each point P of M there is a neighborhood of P such that every locally connected subcontinuum is a dendrite.*

Proof. Suppose $K_1{}^0$ is locally compact, but that in each of the neighborhoods U_i closing down on P there is a locally connected subcontinuum which is not a dendrite. Thus there is a simple closed curve C_i in each U_i and $\delta(C_i) \to 0$. This of course implies that $[C_i] \underset{0}{\to} P$. Now corresponding to any neighborhood U_p of p there exists a number n such that $K_0{}^1 \cdot K_1{}^0 \cdot h_K(C_n) \subset U_p$. For if this were not so there would be an arc P_i of C_i such that $p_i \epsilon C(U_p)$. Again $\delta(P_i) \to 0$; and hence $[P_i] \underset{\leqq r}{\to} P$; that is, $[p_i] \to p$. But this is impossible since $C(U_p)$ is closed and $p \epsilon U_p$. Now consider the set $K_0{}^1 \cdot K_1{}^0 \cdot h_K(C_n) \subset U_p$. This set consists of all subarcs of the simple closed curve C_n and hence contains a convergent sequence of arcs no subsequence of which converges 0-regularly. This subsequence generates a subset of U_p which has no limit point, hence U_p is not compact. But U_p was any neighborhood of p, hence the local compactness at p is violated.

The following two corollaries follow immediately.

COROLLARY 7.61. *If K is locally compact, then the conclusion of Theorem 7.6 holds.*

COROLLARY 7.62. *If M is locally connected and K_1^0 (or K) is locally compact, then M is locally a dendrite.*

THEOREM 7.7. *If M is locally a dendrite, then K_1^0 is locally compact.*

Proof. The hypothesis that M be locally a dendrite implies that every component of M contain only a finite number of true cyclic elements each one of which is a linear graph. Thus M contains only a finite number of simple closed curves. Now consider any p in K; hence P is a locally connected continuum. We can find an ϵ-neighborhood of P whose closure contains those simple closed curves of M and only those contained in P. Denote by L the subset of K_1^0 corresponding to the collection of locally γ^s $(s \leqq r)$ connected subcontinua of $U_\epsilon(P)$ which contain all the true cyclic elements of P. L is open for if not there would be a sequence $[P_i] \underset{\leqq r}{\rightarrow} P$, where we can suppose all the P_i are in $U_\epsilon(P)$, but each P_i does not contain at least one point of some simple closed curve of P. But G. T. Whyburn has shown [17] that every simple closed curve of P would have to be the 0-regular limit of a sequence of simple closed curves in the $[P_i]$. Thus since the total number of simple closed curves is finite, almost all $[P_i]$ would have to contain the simple closed curves of P contrary to hypothesis.

Finally $\bar{L}$ is compact. To see this consider the following decomposition G of M. The set g will be an element of G if it is a true cyclic element of a component of M or a point not contained in one. This decomposition is upper semi-continuous since the number of true cyclic elements is finite. Let M' be the hyperspace associated with the decomposition. Clearly each component of M' is a dendrite. Now consider any infinite sequence of points $[p_i]$ in $\bar{L}$; that is, a sequence $[P_i]$ each one of which contains the same simple closed curves as P. Suppose $[P_{n_i}]$ is a convergent subsequence with limit P, and $[P'_{n_i}]$ are the corresponding sets in M', then $[P'_{n_i}] \underset{\leqq r}{\rightarrow} P'$ since all sets are subsets of a dendrite. This implies the regular convergence of $[P_{n_i}]$ since the elements of the decomposition of M which are not points are all fixed in the convergence, and hence $[p_{n_i}] \rightarrow p$.

This shows the local compactness of K_1^0 at p, for if V_p is any neighborhood of p, then there is a neighborhood W_p such that $\overline{W}_p \subset V_p$. Also $W_p \cdot L$ is open and $\overline{W_p \cdot L} \subset \overline{W}_p \cdot \bar{L}$ is a compact subset of V_p.

THEOREM 7.8. *$K_{n,0,0,\ldots,0}$ $(n > 1)$ will be complete if and only if M is finite.*

---

[17] See reference in footnote [16], p. 413.

Proof. The proof follows the same pattern as Theorem 7.2 except that here we must show that $[A_i]$ is a Cauchy sequence, $A_i = a_i + a_{i+1} + \cdots + a_{i+n}$. This follows immediately from the fact that the $f_{ij}(A_k) = 0$ for as many of the i and j as we wish and for almost all k, where the f_{ij} are the functions used in defining the metric.

The following two corollaries are immediate.

COROLLARY 7.81. *If $n > 1$, a necessary and sufficient condition that $K_n{}^0$ be complete is that M be finite.*

COROLLARY 7.82. *A necessary and sufficient condition that $K_1{}^0$ be complete is that M be finite.*

THEOREM 7.9. *If M is locally connected, a necessary and sufficient condition that $K_1{}^0$ be complete is that every component of M be a dendrite.*

Proof. The proof follows the same pattern as Theorem 7.8 and follows from the fact that a sequence of subarcs of a simple closed curve which converges to the simple closed curve is a Cauchy sequence.

Thus the hypothesis of completeness imposes about the same restrictions on K as does compactness.

UNIVERSITY OF VIRGINIA
AND
LOUISIANA STATE UNIVERSITY.

UNIVERSAL FUNCTIONS OF POLYGONAL NUMBERS, II.*

By L. W. Griffiths.

1. Introduction. The universal functions of polygonal numbers of order $m+2$, with the sum of the coefficients in each function equal to $m+3$, are determined in this paper. If the sum of the coefficients is at most $m+2$ the universal functions have been determined.[1] A necessary and sufficient condition that the universality of a function of weight $m+3$ be not implied by that of a function of weight at most $m+2$ is proved. For each $m \geqq 3$ a universal function of weight $m+3$ satisfying this condition is exhibited.

The general development of this paper is suggested by the paper to which reference has been made. Certain notations and facts established in that paper are used. Many proofs are so similar that they are not presented here.

The polygonal numbers of order $m+2$ are defined, for m a positive integer, by $p(x) = x + m(x^2 - x)/2$ with $x = 0, 1, 2, \cdots$. Here $m \geqq 3$, for the reasons stated in I. The coefficients $a_1, \cdots, a_n$ in the functions $f = (a_1, \cdots, a_n) = a_1p_1 + \cdots + a_np_n$ are positive integers to be determined. Also $1 \leqq a_1 \leqq \cdots \leqq a_n$, and, by definition, $w_k = a_1 + \cdots + a_k$ $(1 \leqq k \leqq n)$ and $w = w_n$. It will be proved that, if $w = m + 3 \geqq 6$, then f is universal only if f satisfies (7), (8), (9), or (10). It will also be proved that f is universal if f satisfies (7), (8), or (10). If f satisfies (9) then f represents every positive integer A except perhaps when $140m + 62 < A < M$, where M depends only on m and f. M is evaluated in Theorem 4. The methods of this paper are applicable to the verification that f actually represents these integers A. Verification is practically certain, but the extremely arduous verification was not carried beyond $140m + 62$.

2. Necessary and sufficient conditions that f represent integers less than $8m+9$. The following lemmas and theorems have been proved by methods similar to those used in the proofs of the corresponding facts in I.

Lemma 1. *Let $w = m+3$. Then $f = 0, \cdots, m+3$ if and only if $f = (1, a_2, \cdots, a_n)$ and $a_k \leqq w_{k-1} + 1$ $(2 \leqq k \leqq n)$.*

* Received October 30, 1942.

[1] L. W. Griffiths, *Annals of Mathematics*, vol. 31 (1930), pp. 1-12. This paper will be cited as I. A misprint is corrected here.

LEMMA 2. *Let $w = m + 3$. Then $f = m + 3, \cdots, 2m + 3$ if and only if $f = (1, 1, a_3, \cdots, a_n)$ and $a_k \leqq w_{k-1}$ $(3 \leqq k \leqq n)$.*

LEMMA 3. *If $m \geqq 4$ and $w = m + 3$, then $f = 2(m + 2), \cdots, 3m + 2$ if and only if f satisfies* (1) *or* (2):

$$(1) \quad f = (1, 1, a_3, \cdots, a_n), \qquad a_k \leqq w_{k-1} - 1 \ (3 \leqq k \leqq n),$$

$$(2) \quad f = (1, \cdots, 1, 2, a_{t+1}, \cdots, a_n), \quad a_k \leqq w_{k-1} - 1 \ (2 \leqq t < k \leqq n).$$

Theorem 1 follows from Lemmas 1, 2, and 3, if $m \geqq 4$; if $m = 3$ it follows from Lemmas 1 and 2, and direct verification for the integers $2(m + 2), \cdots, 3m + 3$.

THEOREM 1. *Let $w = m + 3 \geqq 6$. Then $f = 0, \cdots, 3m + 3$ if and only if f satisfies* (3) *or* (4):

$$(3) \quad f = (1, 1, 1, 3)$$

$$(4) \quad f = (1, 1, a_3, \cdots, a_n), \ a_3 = 1, 2, \ a_k \leqq w_{k-1} - 1 \ (4 \leqq k \leqq n).$$

If f satisfies (4) with $a_3 = 1$, then $f = 3m + 3, \cdots, 5m + 6$. If f satisfies (3) then $f \neq 4m + 7$. If f satisfies (4) with $a_3 = 2$, and if there exists a coefficient a_h such that $a_h = w_{h-1} - 1 > 3$, then $f \neq 4m + 6 + a_h + \cdots + a_n$. But if no such coefficient a_h exists then $f = 3m + 3, \cdots, 5m + 6$. These facts prove Theorem 2.

THEOREM 2. *Let $w = m + 3 \geqq 6$, then $f = 0, \cdots, 5m + 6$ if and only if f satisfies* (5) *or* (6):

$$(5) \quad f = (1, 1, 1, a_4, \cdots, a_n), \ a_k \leqq w_{k-1} - 1 \ (5 \leqq k \leqq n),$$

$$(6) \quad f = (1, 1, 2, a_4, \cdots, a_n), \ a_4 = 2 \text{ or } 3, \ n = 4 \text{ or } a_k \leqq w_{k-1} - 2 \ (5 \leqq k \leqq n).$$

If f satisfies (6) with $a_4 = 3$ and $n > 4$, or if f satisfies (5) with $a_4 = 1$ and $a_5 = 3$ and $n > 5$, then $f \neq 5m + 9$. Otherwise the functions (5) and (6) represent the integers $5m + 7, \cdots, 8m + 8$, except that $(1, 1, 2, 3) \neq 7m + 10$. These facts prove Theorem 3.

THEOREM 3. *Let $w = m + 3 \geqq 6$. Then $f = 0, \cdots, 8m + 8$ if and only if f satisfies* (7), (8), (9), *or* (10):

$$(7) \quad f = (1, 1, 1, 1, a_5, \cdots, a_n), \quad a_k \leqq w_{k-1} - 1 \ (5 \leqq k \leqq n), \text{ and } a_5 \neq 3 \text{ if } n > 5,$$

(8) $f = (1, 1, 1, 2, a_5, \cdots, a_n), \quad a_k \leqq w_{k-1} - 1 \; (5 \leqq k \leqq n),$

(9) $f = (1, 1, 2, 2, a_5, \cdots, a_n), \quad a_k \leqq w_{k-1} - 2 \; (5 \leqq k \leqq n),$

(10) $f = (1, 1, 2, 2).$

3. Universality of the functions in Theorem 3. To prove that a function f which satisfies (7) with $a_5 = 1$ represents every positive integer it is sufficient, by Theorem 3, to establish Theorem 4 and to verify that, if A is an integer such that $8m + 8 < A < 44m + 40$, then A is represented by f. Further details in the proofs of Theorem 4 and 5 are not presented here, except to remark that the proof of Theorem 4, if f satisfies (9) or (10), uses auxiliary lemmas proved by Dickson [2] and by myself.[3]

THEOREM 4. *Let f satisfy Theorem 3. Then there is an integer M, depending only on m and f, such that f represents every integer $\geqq M$. If f satisfies (7) with $a_5 = 1$, then $M = 44m + 40$; if f satisfies (7) with $a_5 = 2$ or 3, then $M = 142m + 208$; if f satisfies (8), then $M = 387m + 108$; if f satisfies (9) or (10), then $M = (11d^2 - 55d + 74)m + (22d - 70)$, where $d = 6, 8, 10, 12, 14, 16$ according as f is $(1, 1, 2, 2)$, $(1, 1, 2, 2, 2)$, $(1, 1, 2, 2, 3, \cdots)$ or $(1, 1, 2, 2, 2, 3, \cdots)$, $(1, 1, 2, 2, 4, \cdots)$ or $(1, 1, 2, 2, 2, 4, \cdots)$, $(1, 1, 2, 2, 2, 5, \cdots)$, $(1, 1, 2, 2, 2, 6, \cdots)$.*

THEOREM 5. *If f satisfies (7), (8), or (10), then f is universal. If f satisfies (9), then f represents every positive integer A except perhaps when $140m + 62 < A < M$.*

4. Universality not implied by that of a function of weight $m + 2$. Theorem 5 and the universal functions of weight at most $m + 2$, found in I, show that a function of weight $m + 3$ has its universality implied by that of a function of lower weight if, and only if, the coefficients of the function of weight $m + 3$ are obtained from the coefficients of a universal function of weight $m + 2$ by adjoining a coefficient 1. No function (8), (9), or (10) can be so obtained. The list of universal functions when $w = m + 2$ omitted the function $(1, 1, 1, 1, 3)$. Hence a function (7) can be so obtained if and only if either it is $(1, 1, 1, 1, 1, 3)$, or it is one of the functions $(1, 1, 1, 1, 2, \cdots)$ with $n \geqq 5$ which does not have a coefficient a_h such that $a_h = w_{h-1} - 1$, or

---

[2] L. E. Dickson, *American Journal of Mathematics*, vol. 56 (1934), pp. 513-528.

[3] L. W. Griffiths, *American Journal of Mathematics*, vol. 55 (1933), pp. 102-110, and vol. 58 (1936), pp. 769-782.

it is one of the functions $(1, 1, 1, 1, 1, 1, \cdots)$ with $n \geqq 6$ which does not have such a coefficient a_h, or it is one of the functions $(1, 1, 1, 1, 1, 2, \cdots)$ with $n \geqq 6$ which does not have such a coefficient a_h.

THEOREM 6. *The universality of a function of weight* $m + 3$ *is not implied by that of a function of weight* $m + 2$ *if and only if it satisfies* (8), *or* (9), *or* (10), *or if it is one of the functions* (7) *which is not in the preceding list.*

If $m \geqq 10$ the function f defined as follows satisfies Theorem 6. Define q and r by $m - 2 = 4q + r$, with $0 \leqq r \leqq 3$, and let $a_1 = \cdots = a_5 = 1$, $a_6 = \cdots = a_{q+4} = 4$, $a_{q+5} = r + 4$. If $m = 3, \cdots, 9$ the following functions, respectively, satisfy Theorem 6, since they satisfy (8): $(1, 1, 2, 2)$, $(1, 1, 1, 2, 2)$, $(1, 1, 1, 2, 3)$, $(1, 1, 1, 2, 4)$, $(1, 1, 1, 2, 2, 3)$, $(1, 1, 1, 2, 3, 3)$, $(1, 1, 1, 2, 3, 4)$.

NORTHWESTERN UNIVERSITY.

THE PROJECTIVE THEORY OF SURFACES IN RULED SPACE, II.*

By Chenkuo Pa.

PART C.

Asymptotic Ruled Surfaces R_1 and R_2.

1. General theory. Consider on a surface S a curve C_t through a point P; the direction of the tangent PT is determined by the value du/dv.[1] The tangents of the asymptotic curves $v = \text{const.}$ ($u = \text{const.}$) drawn from the points of C_t constitute a ruled surface known as the asymptotic ruled surface $R_1(R_2)$ of S along C_t. In order to discuss the behavior of these ruled surfaces in the neighborhood of the given point P, it is convenient for us first to determine in our coördinate system the fundamental quantities at P. For the subsequent discussion we notice here two sets of formulas.

It is clear that the non-homogeneous coördinates of an ordinary point $(\bar{x})$ of R_1 are of the form (6), so that the differential equation of the curved asymptotic lines are given by the expression (7). Our purpose is to normalize the coördinates of $(\bar{x})$ so that the condition (3) should be satisfied at P. To this end, we introduce at the given point a transformation defined by

$$x' = x + (\beta t^2)_0 z, \qquad y' = y - (\beta t)_0 z. \tag{67}$$

It is readily seen that the fundamental differential equations (1) remain unaltered and at P

$$x'_u = y'_v = z'_{uv} = 1,\ y'_u = z'_u = x'_v = z'_v = 0,\ x'_{uv} = \beta t^2,\ y'_{uv} = -\beta t. \tag{68}$$

Since after this substitution the point $(\bar{x})$ may be written in the same form as (6), namely,

$$\bar{x} = \lambda x_u + x = \lambda x'_u + x',$$

the differential equation (7) of the curved asymptotic lines of R_1 also remains unaltered. Since the fundamental differential equation of R_1 must be com-

* Received June 1, 1942. Parts A and B of this paper appeared in this Journal, vol. 65 (1943), pp. 712-736.

[1] We denote, for brevity, du/dv by t, d^2u/dv^2 by t', the osculating plane to C_t at P by π_t and the tangent plane to S at P by π etc.

pletely integrable we can introduce a new asymptotic parameter w in place of λ such that at P

$$(69)\qquad (\partial\lambda/\partial w)_0 = 1. \qquad (\partial^2\lambda/\partial w^2)_0 = \theta_u.^2$$

The advantage of choosing w in this way is that the conditions (3) still hold for R_1 at P, so that

$$(70)\qquad \bar{x}_w = \bar{y}_v = \bar{z}_{wv} = 1, \quad \bar{x}_w = \bar{y}_w = \bar{z}_v = \bar{z}_w = \bar{x}_{wv} = \bar{y}_{wv} = 0.$$

For the sake of convenience (x') is replaced by (x) and therefore (68) by the following

$$(68')\qquad x_u = y_v = z_{uv} = 1, \; y_u = x_v = z_u = z_v = 0, \; x_{uv} = \beta t^2, \; y_{uv} = -\beta t.$$

After this reduction the method which we have so far used for the computation of the fundamental quantities of $Q_u{}^h$ is applicable, without any alteration, to the surface R_1. Let the fundamental differential equations of R_1 be

$$\bar{x}_{ww} = \theta_{1w}\bar{x}_w + \beta_1\bar{x}_v, \quad \bar{x}_{uv} = \theta_w\bar{x}_v + \gamma_1\bar{x}_w;$$

then we can easily show that at P

$$\theta_{1w} - (\partial^2\lambda/\partial w^2)/(\partial\lambda/\partial w) = \theta_u, \quad \beta_1 = 0.$$

Putting, for brevity,

$$N = \theta_{uv} + \beta\gamma + 2\beta_v t + (\beta_u - \beta\theta_u)t^2 + \beta t' + \beta t(\theta_v - \beta t^2),$$

we have the differential equation (7) in the form

$$\lambda_v = \tfrac{1}{2}\lambda^2 N - \lambda(\theta_u t + \beta t^2) - t.$$

Now, denote by X_v the derived function of a function X ($X \neq x, y, z, \beta, \gamma, \theta_u, \theta_v$ etc.) along a curved asymptotic line of R_1; by virtue of the equation (7) we have

$$\bar{x}_v = l x_u + m x_v + \lambda x_{uv},$$

where the quantities l, m are given by

$$l = \lambda\theta_u t + t + \lambda_v = \tfrac{1}{2}\lambda^2 N - \lambda\beta t^2, \quad m = 1 + \lambda\beta t.$$

In order to calculate the fundamental quantities of R_1, it is useful to establish here some relations at P:

---

[2] For the following discussion it is unnecessary to choose the values of $\partial^m\lambda/\partial w^m$ (for $m \geqq 3$) at P.

$$\lambda_v = -t, \quad \lambda_{vw} = -\theta_u t - \beta t^2, \quad \lambda_{vv} = \theta_u t^2 + \beta t^3 - t',$$
$$\lambda_{wwv} = N - \theta_u{}^2 t - \beta\theta_u t^2,$$
$$\lambda_{wvv} = -tN - (\theta_{uu}t^2 + \theta_{uv}t + \theta_u t' + 2\beta t t' + \beta_u t^3 + \beta_v t^2) + (\theta_u + \beta t)^2 t^2,$$
$$m = 1, \quad m_v = -\beta t^2, \quad m_w = \beta t, \quad m_{vw} = -\beta^2 t^3 + (\beta_u - \beta\theta_u)t^2 + \beta_v t + \beta t',$$
$$m_{uv} = \beta\theta_u t^3 + \beta^2 t^4 - 3\beta t t' - 2\beta_u t^3 - 2\beta_v t^2,$$
$$l = 0, \quad l_v = \beta t^3, \quad l_w = -\beta t^2,$$
$$l_{vw} = \beta\theta_u t^3 + \beta^2 t^4 - tN - 2\beta t t' - \beta_u t^3 - \beta_v t^2,$$
$$l_{vv} = t^2 N - \lambda_{vv}\beta t^2 + 2\beta_u t^4 + 2\beta_v t^3 + 4\beta t^2 t'.$$

By means of the identity $\theta_{uv} = (\partial^2\lambda/\partial w^2)/(\partial\lambda/\partial w)$ we obtain at P

$$\theta_{1wv} = \lambda_{wwv} + \theta_u{}^2 t + \beta\theta_v t^2.$$

Substituting the value of λ_{wwv} at P in the right-hand side of this equation we have at P

$$\theta_{1wv} = N.$$

Differentiation of $\bar{x}_v$ along the curved asymptotic line of R_1 at P yields the relations

$$\bar{x}_{vv} = (\gamma + \beta t^3)x_u + (\theta_v - \beta t^2)x_v.$$

On the other hand, the fundamental differential equations give

$$\bar{x}_{vv} = \theta_{1v}\bar{x}_v + \gamma_1\bar{x}_w.$$

Taking account of the values of $(\bar{x}_v)$, $(\bar{x}_w)$ and (x_u), (x_v) given by (70) and (68′) we have the two following relations:

$$\gamma_1 = \gamma + \beta t^3, \qquad \theta_{1v} = \theta_v - \beta t^2.$$

After a simple calculation we find the values of $(\bar{x}_{vvv})$ at P as follows:

$$\begin{aligned}\bar{x}_{vvv} = {} & [l_{vv} + 2l_v\theta_u t + \gamma_v + \gamma\theta_v + 2\gamma m_v - t^2(\theta_{uv} + \beta\gamma)]x_u \\ & + (2l_v + t' + \gamma + 2m_v t + \lambda_{vv} - \theta_u t^2)x_{uv} + (*)x_v,\end{aligned}$$

and on the other hand by using the differential equation we have that at P

$$\bar{x}_{uvv} = (\gamma_{1v} + \gamma_1\theta_{1v})\bar{x}_w + (*)\,\bar{x}_v + (*)\,\bar{x}_{wv}.$$

Use of (70) and (68′) gives one of the required relations, namely, at P

$$\gamma_{1v} = \gamma_v + 3\beta_u t^4 + 4\beta_v t^3 + 6\beta t^2 t'.$$

Moreover, the value of $(\bar{x}_{vvw})$ at P may be represented as follows

$$\bar{x}_{vvw} = [l_{vw} + l_w + \theta_u + m_w\gamma + \lambda_w t(\theta_{uv} + \beta\gamma) + \lambda_w(\gamma_u + \gamma\theta_u)]x_u \\ + (l_w + m_w t + \lambda_{vw} + \lambda_w\theta_u t + \lambda_w\theta_v)x_{uv} + (*)\, x_v.$$

If we differentiate the fundamental differential equations for $(\bar{x})$ we have

$$\bar{x}_{vvw} = (\gamma_{1w} + \gamma_1\theta_{1w})\bar{x}_w + (*)\ \bar{x}_v + (*)\ \bar{x}_{vw}.$$

Therefore

$$\gamma_{1w} = \gamma_u + \beta\gamma t + \beta^2 t^4 - 3\beta_v t^2 - 2\beta_u t^3 - 3\beta t t'.$$

Thus we have obtained the fundamental quantities of the surface R_1 at the given point P up to and including the neighborhood of order 4 of the surface. In summary, we have the following formulas:[3]

$$(71)\quad \begin{cases} \beta_1 = 0, \quad \gamma_1 = \gamma + \beta t^3, \quad \theta_{1u} = \theta_u, \quad \theta_{1v} = \theta_v - \beta t^2, \\ \gamma_{1u} = \gamma_u + \beta\gamma t + \beta^2 t^4 - 3\beta_v t^2 - 2\beta_u t^3 - 3\beta t t', \\ \gamma_{1v} = \gamma_v + 3\beta_u t^4 + 4\beta_v t^3 + 6\beta t^2 t', \\ \theta_{1uv} = \theta_{uv} + \beta\gamma + 2\beta_v t + (\beta_u - \beta\theta_u)t^2 + \beta t' + \beta\theta_v t - \beta^2 t^3. \end{cases}$$

It remains to determine the relations between the second order of a curve C_t when it is referred to the coördinate systems defined by S and by R_1, respectively, at P.[4] According as the curve C_t is referred to the coördinate system of S or R_1 the equation of the osculating plane π_t of C_t is given by

$$2t^2 y - 2tx - (\beta t^3 - \gamma + t\theta_v - t^2\theta_u - t')z = 0$$

or

$$2t_1^2 y_1 - 2t_1 x_1 - (\beta_1 t_1^3 - \gamma_1 + \theta_{1v} t_1 - \theta_{1u} t_1^2 - t'_1)z_1 = 0,$$

where

$$(72)\qquad x_1 = x + \beta t^2 z, \quad y_1 = y - \beta t z, \quad z_1 = z,$$

and t_1, t'_1 are the corresponding values of t and t' of C_t in the new system of reference. From the relation (72), it is evident that $t_1 = t$, so that the condition for the equivalence of these two equations is

$$t'_1 = t' + \beta t^3.$$

Thus we have

$$(73)\qquad t_1 = t, \quad t'_1 = t' + \beta t^3,$$

and conclude that *the equation of any geometrical element of R_1 defined by the neighborhood of fourth order at P may be found by applying the trans-*

[3] In the following we write, for the sake of convenience, u in place of w.

[4] We define a coördinate system of R_1 at P in a similar manner as that of S.

formation (71), (72) *and* (73) *to the corresponding equation of the same element defined by S in our system of reference.* As an illustration, taking the equation of the osculating quadric of R_1 at P

$$x_1y_1 - z_1 - \tfrac{1}{2}\theta_{1uv}z_1^2 = 0,$$

and making use of the method just mentioned, we find the equation of one of the asymptotic osculating quadrics of S associated with C_t as was shown in Part A.

The corresponding values of the fundamental quantities β_2, γ_2, θ_{2u}, θ_{2v} etc., of R_2 may be obtained by interchanging in the equation (71) the quantities u and v; β and γ; t and t^{-1}; t' and $-t^{-3}t'$ etc. We do not write them here in full. For the following discussion we put

$$(74)\qquad \begin{cases} P_1 = \gamma_{1u}/\gamma_1 + \theta_{1u}, & P_2 = \beta_{2v}/\beta_2 + \theta_{2v}, \\ Q_1 = 2\theta_{1v} - \gamma_{1v}/\gamma_1, & Q_2 = 2\theta_{2u} - \beta_{2u}/\beta_2, \end{cases}$$

and

$$(75)\qquad \begin{cases} \phi_1 = \gamma_u/\gamma + \theta_u, & \phi_2 = 2\theta_u - \beta_u/\beta, \\ \psi_1 = \beta_v/\beta + \theta_v, & \psi_2 = 2\theta_v - \gamma_v/\gamma. \end{cases}$$

2. A pencil of lines associated with a curve on a surface. In the present section we define a pencil of invariant lines which characterize the second order of a curve C_t of S. It is well known that by means of the second order of a space curve we can not define any element other than the osculating plane. Here we shall define other elements by making use of the relations between the curve and the surface.

The expansions of the curved asymptotic line C_1 of R_1 at P are known to be

$$\begin{cases} x_1 = \tfrac{1}{2}\gamma_1y_1^2 - \tfrac{1}{6}\gamma_1Q_1y_1^3 + C_1y_1^4 + (5), \\ z_1 = \tfrac{1}{6}\gamma_1y_1^3 - \tfrac{1}{12}\gamma_1Q_1y_1^4 + (\tfrac{3}{5}C_1 - \tfrac{1}{60}\gamma_1^2\phi_1)y_1^5 + (6). \end{cases}$$

With the aid of the transformation (72) the above equations can be written in the form

$$(76)\qquad \begin{cases} x = \tfrac{1}{2}\gamma_1y^2 - \tfrac{1}{6}\gamma_1(Q_1 + \beta t^2)y^3 + (C_1 + \tfrac{1}{12}\beta\gamma_1Q_1t^2)y^4 + (5), \\ z = \tfrac{1}{6}\gamma_1y^3 - \tfrac{1}{12}\gamma_1Q_1y^4 + (\tfrac{1}{12}\beta\gamma_1^2t + \tfrac{3}{5}C_1 - \tfrac{1}{60}\gamma_1^2\phi_1)y^5 + (6), \end{cases}$$

where Q_1, ϕ_1 are defined in (74) and (75) respectively and

$$C_1 = \tfrac{1}{24}\{\gamma_1(-2\theta_{1vv} + 6\theta_{1v}^2 + \gamma_1\theta_{1u} + \gamma_{1u}) + \gamma_{1vv} - 5\gamma_{1v}\theta_{1v}\}.$$

Similar expansions may be obtained for the curved asymptotic line C_2 of R_2

by interchanging in (76) the quantities x and y; u and v; β and γ; Q_1 and Q_2 and the indices 1 and 2, etc.

From (71) it follows immediately that when C_t touches a Darboux tangent at P then the asymptotic curve C_1 has a point of inflection at P and consequently that any Darboux curve is a flecnode curve of its asymptotic ruled surfaces R_1 and R_2, as has been pointed out by Palozzi.[5] In fact, both the asymptotic ruled surfaces R_1, R_2 associated with C_t and the given surface S have at P equal projective linear elements in the direction t, since

$$\begin{aligned}\tfrac{1}{2}\gamma_1(dv^2/du) &= \tfrac{1}{2}(\gamma + \beta(du/dv)^3)(dv^2/du) \\ &= (\gamma dv^3 + \beta du^3)/2dudv = \tfrac{1}{2}\beta_2(du^2/dv).\end{aligned}$$

Moreover, the contact invariant of C_1 with respect to the asymptotic curve v of S at P is equal to $\gamma_1/\gamma = 1 + (\beta/\gamma)(du/dv)^3$ which has been interpreted by Bompiani as the contact invariant of two certain conics.[6]

Obviously, the curves C_1 and C_2 have a common osculating plane at P. According to Bompiani there are three principal points determined by this pair of curves[7] and in this case they are collinear. The straight line containing them will be called the *second principal line of C_t at P*, and the dual line in the correspondence of Bompiani[8] the *first principal line of C_t at P*. After a simple calculation we find the equations of the second principal line, namely,

$$\tfrac{1}{4}Q_2x + \tfrac{1}{4}Q_1y + 1 = 0, \quad z = 0, \tag{77}$$

and those of the first principal line

$$x + (\tfrac{1}{4}Q_1 + \beta t^2)z = 0, \quad y + (\tfrac{1}{4}Q_2 + \gamma t^{-2})z = 0. \tag{78}$$

We can now prove the following

THEOREM. *The pangeodesic of a surface is characterized by the property that the first principal line at every point lies on the osculating plane at the same point.*

---

[5] G. Palozzi, "Una proprietà caratteristica delle tangenti di Darboux," *Rendiconti dei Lincei*, (*VI*), vol. 13 (1931), pp. 483-488.

[6] E. Bompiani, "Gli invarianti proiettivi nella teoria delle superficie, I—Ricostruzione rapida della teoria delle applicabilità proiettive," *Rendiconti dei Lincei* (VI), vol. 24 (1936), pp. 323-332.

[7] E. Bompiani, "Invarianti d'intersezione di due curve schembe," *Rendiconti dei Lincei*, (VI), vol. 14 (1931), pp. 456-461.

[8] Cf. Buchin Su, "On the intersection of two curves in space," *Tôhoku Math. Journ.*, vol. 39 (1934), pp. 226-232.

As a curve on a surface in metric space is a geodesic when and only when the osculating plane passes through the surface normal at the same point, the above definition for pangeodesics furnishes a generalization in projective geometry.

Moreover we have the following theorem:

When the curve C_t varies but remains tangent to a given tangent direction t, the second principal line always passes through a fixed point. This point lies on t when and only when t is a tangent of Segre, and then the polar line of P with respect to the triangle formed by three points corresponding to three tangents of Segre is the second projective normal. Dually, the locus of the first principal line is a plane. This plane passes through t when and only when t is a Segre tangent and then the polar line of the tangent plane π with respect to the trihedron formed by three planes corresponding to three tangents of Segre is the first projective normal.

The second order of a curve of Segre satisfies the following differential equations

$$t' = \tfrac{1}{3}[t^2(\gamma_u/\gamma - \beta_u/\beta) + t(\gamma_v/\gamma - \beta_v/\beta)], \quad t = w^i\sqrt[3]{(\gamma/\beta)}, \quad (i = 1, 2, 3)$$

where $\omega^3 = 1$ and $\omega \neq 1$. By using these equations we prove the following result:

The first principal lines of three Segre curves through P form a trihedron with respect to which the polar line of the tangent plane of S at P is the first canonical line $c(-\frac{1}{8})$.[9]

Consider the osculating linear complex l_1 of C_1 at P whose equation is

$$p'_{12} - p'_{34} + P_1 p'_{13} = 0,$$

where the quantities (p'_{ij}) are the Plücker coördinates of a line referred to the coördinate system of R_1 at P. Making use of the relations (72) we have

$$(79) \quad \begin{cases} p'_{12} = p_{12} - \beta t^2 p_{23} - \beta t p_{13}, & p'_{14} = p_{14} + \beta t^2 p_{34}, & p'_{24} = p_{24} - \beta t p_{34}, \\ p'_{13} = p_{13}, & p'_{23} = p_{23}, & p'_{34} = p_{34}. \end{cases}$$

By means of (79) the equation of l_1 is reducible to

[9] For another interpretation of this line cf. my note "On the quadrics of Moutard," appearing in *Univ. Nac. Tucuman Revista, A*, vol. 2 (1941), pp. 67-77.

(80) $$p_{12} - \beta t^2 p_{23} - p_{34} + (P_1 - \beta t) p_{13} = 0.$$

Interchanging the quantities β and γ; u and v; t and t^{-1}; P_1 and P_2 and the indices 1, 2 gives the equation of the asymptotic osculating linear complexes l_2 of C_2 at P, namely,

(81) $$p_{12} + \gamma t^{-2} p_{13} + p_{34} - (P_2 - \gamma t^{-1}) p_{23} = 0.$$

By means of (80) and (81) we find readily the second directrix of l_1 and l_2

(82) $$\tfrac{1}{2}(P_1 - \beta t - \gamma t^{-2})x + \tfrac{1}{2}(P_2 - \gamma t^{-1} - \beta t^2)y + 1 = 0, \quad z = 0,$$

and the first directrix

(83) $$x + \tfrac{1}{2}(P_2 - \gamma t^{-1} + \beta t^2)z = 0, \quad y + \tfrac{1}{2}(P_1 - \beta t + \gamma t^{-2})z = 0.$$

From this equation it follows that *the osculating plane of a curve C_t passes through the first directrix at the same point when and only when the curve C_t is a pangeodesic of S.* Moreover, *the theorem mentioned above is valid if the first principal line is taken in place of the first directrix.*

Let us now consider a pencil formed by the first principal line and the first directrix at P. We shall call such a pencil the *first associate pencil of C_t at P* and its plane the *associate plane.* In a similar way we define in the tangent plane the *second associative pencil* and the *associate point* of C_t.

A ray l_ρ in the first associate pencil may be represented by the equations

(84) $$\begin{cases} x + [1/(1+\rho)][\tfrac{1}{4}Q_1 + \beta t^2 + (\rho/2)(P_2 - \gamma t^{-1} + \beta t^2)]z = 0, \\ y + [1/(1+\rho)][\tfrac{1}{4}Q_2 + \gamma t^{-2} + (\rho/2)(P_1 - \beta t + \gamma t^{-2})]z = 0, \end{cases}$$

which is determined by the directrix l_∞, the principal line l_0 and one value of a certain double ratio. Similarly we have a ray m_ρ in the second associate pencil

(85) $$\begin{aligned}&[1/(1+\rho)][\tfrac{1}{4}Q_2 + (\rho/2)(P_1 - \beta t - \gamma t^{-2})]x \\ &\quad + [1/(1+\rho)][\tfrac{1}{4}Q_1 + (\rho/2)(P_2 - \gamma t^{-1} - \beta t^2)]y + 1 = 0, \quad z = 0.\end{aligned}$$

From the preceding discussion it is readily seen that the associate plane of a curve C_t on the surface becomes the osculating plane when and only when C_t is a pangeodesic.

There are quadrics of a pencil each of which has at P a contact of at least the fourth order both with C_1 and C_2.

(86) $$xy - 3z - (\tfrac{1}{2}Q_2 - \gamma t^{-2})xz - (\tfrac{1}{2}Q_1 - \beta t^2)yz + kz^2 = 0,$$

where k denotes an arbitrary parameter.

It may easily be proved that the projectivity P formed by the product of the null systems of the asymptotic osculating linear complexes of C_1 and C_2 at P is an involution. There exist quadrics of two pencils each of which passes through the asymptotic tangents and remains invariant under the projectivity P. One of these pencils may be represented by

$$xy - z + \gamma t^{-2}xz + \beta t^2 yz + kz^2 = 0, \tag{87}$$

and the other by

$$xy + z + (P_1 - \beta t)xz + (P_2 - \gamma t^{-1})yz + kz^2 = 0. \tag{88}$$

where k denotes a parameter.

We can prove that each regulus of any quadric in the pencil (87) or (88) belongs to one of the two osculating linear complexes l_1 and l_2. The common polar lines of (87) and (88) are directrices of C_t and those of the pencils (86) and (87) are the principal lines. Furthermore the only common polar lines of (86) and (88) in the tangent plane belong precisely to the second associate pencil.

We further remark that a ray of the second associate pencil can be defined by means of the neighborhood of the 5-th order of both the curves C_1 and C_2 at P.

3. New covariant curves on a surface. Having thus discussed the various properties of the directrix and the principal line of a curve or a surface as well as the advantage of introducing them for the definition of pangeodesics, we come to a more general consideration of the associate pencil. In the following lines we shall see that this pencil of lines plays an important rôle in the study of certain covariant curves of a surface.

The polar line of m_ρ in the fundamental polarity is a line whose equations are

$$\begin{cases} x + [1/(1+\rho)][\tfrac{1}{4}Q_1 + (\rho/2)(P_2 - \gamma t^{-1} - \beta t^2)]z = 0, \\ y + [1/(1+\rho)][\tfrac{1}{4}Q_2 + (\rho/2)(P_1 - \beta t - \gamma t^{-2})]z = 0. \end{cases}$$

This line lies in the osculating plane to the curve C_t at P when and only when C_t satisfies the following differential equation

$$\begin{aligned} &- [2t^2/(1+\rho)][\tfrac{1}{4}Q_2 + (\rho/2)(P_1 - \beta t - \gamma t^{-2})] \\ &+ [2t/(1+\rho)][\tfrac{1}{4}Q_1 + (\rho/2)(P_2 - \gamma t^{-1} - \beta t^2)] \\ &= \beta t^3 - \gamma + t\theta_v - t^2\theta_u - t'. \end{aligned}$$

After a simple reduction we can write the above differential equation in the form

$$(89) \qquad (\gamma+\beta t^3)t' = t^2(\gamma_u-\beta_v t^2)+\tfrac{1}{2}t(\gamma_v-\beta_u t^4) \\ +[(1+\rho)/(2\rho-1)](\beta^2 t^6-\gamma^2),$$

which defines a system of curves C_ρ called *the deformable curves.* From this equation, we infer that the Darboux tangents are singular directions for the curves of this system and that only the tangent of Segre has the property that the osculating plane of a curve on S touching this tangent at P must pass through the polar line of $m_{\frac{1}{2}}$ with respect to the quadric of Lie. *For $\rho=-1$ the corresponding curve C_{-1} is a pangeodesic. If the tangent t varies at P the osculating plane to the corresponding deformable curve C_ρ at this point envelops a cone K_ρ of class 6 and, in particular, K_{-1} is the cone of Segre.*

When a one-to-one correspondence of any kind is established between the points of two surfaces, either surface may be said to be represented on the other. Following this definition and noticing that the asymptotic tangents are singular directions for any deformable curve C_ρ other than pangeodesics (i. e. $\rho\neq-1$), we conclude immediately that if two surfaces S and $\bar{S}$ be representable upon each other and if all the deformable curves of two surfaces, other than the pangeodesics, of the same kind be in correspondence, then *all the asymptotic curves of S and $\bar{S}$ must be also in correspondence, and the surfaces are then projectively applicable.* In fact, we can take on S and $\bar{S}$ the same asymptotic parameters (u,v) and the same system of reference we have so far used. Let $\beta,\bar{\gamma}$ correspond on $\bar{S}$ to $\bar{\beta},\gamma$; then the deformable curve $\bar{C}_\rho$ $(\rho\neq-1)$ of $\bar{S}$ may be represented by the following equation

$$(\bar{\gamma}+\bar{\beta}t^3)t' = t^2(\bar{\gamma}_u-\bar{\beta}_v t^2)-\tfrac{1}{2}t(\bar{\gamma}_v-\bar{\beta}_u t^4)+[(1+\rho)/(2\rho-1)](\bar{\beta}^2 t^6-\bar{\gamma}^2),$$

which defines, by hypothesis, C_ρ $(\rho\neq-1)$. Hence we have

$$\bar{\beta}=\beta, \quad \bar{\gamma}=\gamma.$$

Thus we have proved the

THEOREM. *A necessary and sufficient condition that two surfaces should be projectively applicable is that the deformable curves, other than pangeodesics, of the same kind on these surfaces be in correspondence.*

We now derive a new class of covariant curves on a surface so as to characterize the surface under collineations.

The principal quadric of a surface may be represented by

$$xy - 3z - \tfrac{1}{2}\phi_2 xz - \tfrac{1}{2}\psi_2 yz + kz^2 = 0,$$

where ϕ_2, ψ_2 are given by (75) and k denotes an arbitrary constant. The polar line of m_ρ with respect to this quadric is

$$x + \{[3/(1+\rho)][\tfrac{1}{4}Q_1 + (\rho/2)(P_2 - \gamma t^{-1} - \beta t^2)] - \tfrac{1}{2}\psi_2\}z = 0,$$
$$y + \{[3/(1+\rho)][\tfrac{1}{4}Q_2 + (\rho/2)(P_1 - \beta t - \gamma t^{-2})] - \tfrac{1}{2}\phi_2\}z = 0.$$

This line lies in the osculating plane to the curve when and only when

$$(90)\quad [2(5\rho - 4)/(1-2\rho)](\gamma + \beta t^3)t' = 3t(\beta_u t^4 - \gamma_v) + 6t^2(\beta_v t^2 - \gamma_u) + [(1+\rho)/(1-2\rho)](\gamma + \beta t^3)(2t^2\theta_u - 2t\theta_v + t\psi_2 - t^2\phi_2 + 4\beta t^3 - 4\gamma)$$

or

$$(90')\quad 2(5\rho - 4)(\gamma + \beta t^3)(t' + \theta_u t^2 - \theta_v t) = (4 - 5\rho)t(\gamma\psi_2 - \beta\phi_2 t^4) + (1+\rho)t^2(\beta\psi_2 t^2 - \gamma\phi_2) + 6t^2(1-2\rho)(\beta\psi_1 t^2 - \gamma\phi_1) + 4(1+\rho)(\beta^2 t^6 - \gamma^2).$$

In Fubini's coördinates we have

$$(90'')\quad 2(5\rho - 4)(\gamma + \beta t^3)[t' + (\partial \log \beta\gamma/\partial u)t^2 - (\partial \log \beta\gamma/\partial v)t] = [(4 - 5\rho)\gamma + (7 - 11\rho)\beta t^3]t(\partial \log \beta^2\gamma/\partial v) - [(4 - 5\rho)\beta t^3 + (7 - 11\rho)\gamma]t^2(\partial \log \beta\gamma^2/\partial u) + 4(1+\rho)(\beta^2 t^6 - \gamma^2).$$

In particular, when $\rho = 4/5$, the corresponding curves are given by the following equation in Fubini's coördinates:

$$\gamma(\partial \log \beta\gamma^2/\partial u)t^2 - \beta(\partial \log \beta^2\gamma/\partial v)t^4 + 4(\beta^2 t^6 - \gamma^2) = 0,$$

which is independent of the second order of these curves.

A curve L_ρ on the surface defined by the differential equation (90) will be called *a projective curve.* It is remarkable that *the curves L_{-1} are pangeodesics. The osculating planes to all these curves L_ρ (for fixed ρ) through the point P envelope a cone N_ρ of class 6 and, in particular, N_{-1} is the cone of Segre.*

With the aid of the cone N_ρ ($\rho \neq -1$) we may define some new canonical lines.

In a way similar to that we have used for the deformable curves we get immediately the

THEOREM. *A necessary and sufficient condition that two surfaces should be projectively equivalent is that the projective curves of the same kind, other than the pangeodesics, on them be in correspondence.*

We shall discuss the deformable curves and projective curves of a surface on another occasion.

4. The correspondence of Segre. Let us define a certain correspondence by means of the curved asymptotic lines C_1 and C_2 of the ruled surfaces R_1 and R_2.[10] It is easy to show that the correspondence in question is the polarity with respect to the following pencil of quadrics

$$xy - z + \gamma t^{-2} yz + \beta t^2 xz + kz^2 = 0, \tag{91}$$

where k denotes an arbitrary constant. In particular we have the

THEOREM. *The point-plane correspondence of Bompiani defined by the pair of curves C_1 and C_2 at P coincides with that of Segre when the point is taken on the tangent of C_t.*

Concerning the pencil of quadrics (91) we can also establish the following

THEOREM. *If the lines of the regulus on a quadric of the pencil* (91) *intersect the asymptotic tangent $v(u)$, then it must belong to the osculating linear complex of $C_1(C_2)$ at P, and conversely.*[11]

Furthermore we can prove the

THEOREM. *Any quadric of the pencil* (91) *has a double line contact with both the asymptotic ruled surfaces R_1 and R_2 at P.*

5. Some covariant quadrics. In a following paper we propose to discuss the geometry of the sequence of asymptotic ruled surfaces $R_1^{(1)}$, $(R_2^{(1)})$ of $R_1(R_2)$, $R_1^{(2)}(R_2^{(2)})$ of $R_1^{(1)}(R_2^{(1)}), \cdots, R_1^{(n)}(R_2^{(n)})$ of $R_1^{(n-1)}(R_2^{(n-1)})$ etc. associated with the curve C_t. We shall call $R_1^{(n)}(R_2^{(n)})$ *the n-th derived asymptotic ruled surface of $R_1(R_2)$.* A full discussion for the asymptotic chord surfaces will also be given later. Here we give only some covariant quadrics of $R_1(R_2)$ associated with the curve C_t.

One of the two asymptotic osculating quadrics of the surface R_1 associated with C_t at P coincides with the osculating quadric of the surface R_1 and the other one may be found by our preceding method, namely,

---

[10] Cf. Buchin Su, *loc. cit.*

[11] Suppose that two curves C_1 and C_2 intersect at P with the same osculating plane but distinct tangents. If the principal points are collinear, then this theorem is also valid.

$$2t^3(x_1y_1 - z_1) + 2\gamma_1 t x_1 z_1 - 2\gamma_1 t^2 y_1 z_1$$
$$+ [-t^3\theta_{1uv} + \gamma_1\{t'_1 - \gamma_1 - (\gamma_{1v}/\gamma_1 - \theta_{1v})t - (2\gamma_{1u}/\gamma_1 + \theta_{1u})t^2\}]z_1^2 = 0.$$

Making use of the transformations (71), (72) and (73) and reducing, we have the equation of this quadric:

$$2t^3(xy - z) + 2\gamma txz - 2\gamma t^2 yz$$
$$+ [-t^3(\theta_{uv} + \beta\gamma) + \gamma\{t' - \gamma - (\gamma_v/\gamma - \theta_v)t - (2\gamma_u/\gamma + \theta_u)t^2\}z^2 = 0,$$

which is precisely the osculating quadric of the surface R_2 at the point P. Hence we have the

THEOREM. *The two asymptotic osculating quadrics of $R_1(R_2)$ associated with the curve C_t coincide with the osculating quadrics of $R_1(R_2)$ and $R_2(R_1)$ at P.*

At a point P of a surface we can also define two quadrics called the asymptotic chord quadrics, as we have obtained the equations in our system of reference in Part A of this paper. These quadrics intersect in the asymptotic tangents and a conic, whose plane α is found to be

$$(\tfrac{1}{6}\gamma t^{-2} + \tfrac{1}{2}\beta t)x - (\tfrac{1}{2}\gamma t^{-1} + \tfrac{1}{6}\beta t^2)y$$
$$- \tfrac{1}{2}\{\tfrac{1}{3}(\gamma_v - \tfrac{1}{2}\gamma\theta_v)t^{-2} + (\gamma_u + \tfrac{1}{2}\gamma\theta_u)t^{-1} - \tfrac{1}{3}(\beta_u - \tfrac{1}{2}\beta\theta_u)t^2$$
$$- (\beta_v + \tfrac{1}{2}\beta\theta_v)t - \tfrac{1}{2}(\gamma t^{-3} + \beta)t'\}z = 0.$$

If we vary the curve C_t but keep it tangent to the tangent t, the locus of the line of intersection of the plane α and the osculating plane π_t of C_t at P is a plane β. In particular, for each tangent of Segre at P the plane β always passes through the new canonical line $c(-2/5)$.

It remains to determine the equation of the asymptotic chord quadrics of the surface $R_1(R_2)$ at P. It is evident that one of these quadrics coincides with the osculating quadric of R_1 and the other may be represented by the following equation:

$$x_1y_1 - z_1 - \tfrac{1}{2}\gamma_1 t^{-1}y_1z_1 + \tfrac{1}{6}\gamma_1 t^{-2}x_1z_1$$
$$- \tfrac{1}{2}\{\theta_{1uv} + \tfrac{1}{3}(\gamma_{1v} - \tfrac{1}{2}\gamma_1\theta_{1v})t^{-2} + (\gamma_{1u} + \tfrac{1}{2}\gamma_1\theta_{1u})t^{-1} - \tfrac{1}{2}\gamma t^{-3}t'_1\}z_1^2 = 0,$$

By means of the method we have so far used the required equation is found to be

$$(92)\quad xy - z + \tfrac{1}{2}(\beta t^3 - \gamma)t^{-1}yz - \tfrac{1}{6}(5\beta t^3 - \gamma)t^{-2}xz$$
$$- \tfrac{1}{2}\{\tfrac{1}{3}\beta\gamma + \theta_{uv} - \tfrac{1}{2}(\gamma t^{-3} + \beta)t' + \tfrac{1}{3}\beta^2t^3 + \tfrac{1}{3}\beta_v t$$
$$- \tfrac{1}{2}\beta\theta_u t^2 + \tfrac{5}{6}\beta\theta_v t + \tfrac{1}{3}\gamma_v t^{-2} - \tfrac{1}{6}\gamma\theta_v t^{-2} + (\gamma_u + \tfrac{1}{2}\gamma\theta_u)t^{-1}\}z^2 = 0.$$

It is readily seen that this quadric is independent of the second order of C_t when and only when the curve C_t touches a Darboux tangent at P and the three corresponding quadrics have a common point on the following line:

$$y + \tfrac{1}{2}\phi z = 0, \quad x + \tfrac{1}{3}\psi z = 0.$$

By a suitable substitution we get the equation of the corresponding quadric of the surface R_2. These two chord quadrics have a residue conic of intersection lying on the plane γ. We can prove that γ coincides with the osculating plane of C_t when and only when this curve C_t is a pangeodesic of the surface.

If the curve C_t varies but remains tangent to a tangent t at P, the locus of this residue conic is a quadric

$$\begin{aligned}(93)\quad & 36(xy - z - \tfrac{1}{2}\theta_{uv}z^2) + 12(\beta t^2 - 2\gamma t^{-1})(y + \tfrac{1}{2}\theta_u z)z \\ & + 12(\gamma t^{-2} - 2\beta t)(x + \tfrac{1}{2}\theta_v z)z \\ & - \{3t^3(\beta + \gamma t^{-3})^2 + 3(\beta_u t^2 + 4\beta_v t + 4\gamma_u t^{-1} + \gamma_v t^{-2}\}z^2 = 0,\end{aligned}$$

which belongs to a Moutard pencil.[12] For each tangent of Darboux the corresponding quadric becomes the Moutard quadric.

THE NATIONAL UNIVERSITY OF CHEKIANG,
KWEICHOW, CHINA.

[12] The Moutard pencil has first been defined by Buchin Su and Asajiro Ichida. See their paper: "On certain cones connected with a surface in the affine space," *Japanese Journal of Mathematics*, vol. 10 (1934), pp. 209-216. For another definition of this pencil compare my paper: "On the quadrics of Moutard," *loc. cit.*

A GENERALIZATION OF ASSOCIATE QUADRICS OF A SURFACE.*

By Chenkuo Pa.

At a generic point of an analytic non-ruled surface, a quadric called the associate quadric has been defined by B. Su.[1] The asymptotic curves of a surface belong to linear complexes if, and only if, the associate quadric of the surface is fixed.[2] The equivalence of this quadric and the second quadric ϕ_1 in Godeaux sequence has been pointed out by L. Godeaux.[3] S. Finikoff has given a quite different definition of the same quadric.[4] The object of this note is to generalize the notion of the associate quadric of a surface from the standpoint of view of Finikoff.

1. For the subsequent discussion it is convenient to utilize the normal coördinate system of Cartan[5] at a given point M of a surface. Let $\{MM_1M_2M_3\}$ be such a tetrahedron of reference; then the conditions of immovability of a line (p_{ij})[6] are easily found to be

$$
\begin{aligned}
\partial p_{12}/\partial u &= A^2\beta p_{24} + K(p_{23} - p_{14}),\\
\partial p_{12}/\partial v &= -\gamma p_{13} - (\partial \log \beta/\partial v)p_{12} + A^2(p_{23} - p_{14}) + B^2\gamma p_{24},\\
\partial p_{13}/\partial u &= -\beta p_{12} - (\partial \log \gamma/\partial u)p_{13} - B^2(p_{14} + p_{23}) + A^2\beta p_{34},\\
\partial p_{13}/\partial v &= B^2\gamma p_{34} - \bar{K}(p_{23} + p_{14}),\\
\partial p_{14}/\partial u &= -p_{13} - B^2 p_{24} - K p_{34},\\
\partial p_{14}/\partial v &= -p_{12} - A^2 p_{34} - \bar{K} p_{24},\\
\partial p_{23}/\partial u &= -p_{13} - B^2 p_{24} + K p_{34},\\
\partial p_{23}/\partial v &= p_{12} + A^2 p_{34} - \bar{K} p_{24},
\end{aligned}
$$

---

* Received June 8, 1942.

[1] Buchin Su, "On the surfaces whose asymptotic curves belong to linear complexes II," *Tôhoku Math. Journ.*, vol. 40 (1935), pp. 433-448.

[2] Buchin Su, *loc. cit.*

[3] L. Godeaux, "Remarques sur les quadriques associées aux points d'une surface," *Journ. Chinese Math. Soc.*, vol. 2 (1937), pp. 1-5.

[4] S. Finikoff, "Sur les quadriques de Lie et les congruences de M. Demoulin," *Recueil Math. de Moscou*, vol. 37 (1930), pp. 48-97.

[5] Cf. S. Finikoff, *Comptes Rendus* (1933), pp. 883-885; Buchin Su, *Tôhoku Math. Journ.*, vol. 41 (1935), pp. 203-215.

[6] We denote the Plücker coördinates of a line joining two points (y) and (z) by $p_{ij} = y_i z_j - z_i y_j$ $(i \neq j,\ i, j = 1, \cdots, 4)$ and (y), (z), (p_{ij}) all refer to the local coördinates.

$$\partial p_{24}/\partial u = -p_{14} - p_{23} + (\partial \log \gamma/\partial u) p_{24},$$
$$\partial p_{24}/\partial v = -\gamma p_{34},$$
$$\partial p_{34}/\partial u = -\beta p_{24},$$
$$\partial p_{34}/\partial v = -p_{14} + p_{24} + (\partial \log \beta/\partial v) p_{34},$$

where the quantities K and $\bar{K}$ are defined by

$$2K = \beta\gamma - \partial^2 \log \beta/\partial u\partial v, \qquad 2\bar{K} = \beta\gamma - \partial^2 \log \gamma/\partial u\partial v.$$

The conditions of integrability in this coördinate system take the form

$$\partial A^2/\partial u = K(\partial \log K\beta/\partial v), \qquad \partial B^2/\partial v = \bar{K}(\partial \log \bar{K}\gamma/\partial u),$$
$$A[\partial(A\beta)/\partial v] = B[\partial(B\gamma)/\partial u].$$

For the sake of convenience we put

$$\tfrac{1}{4}N = B[\partial(B\gamma)/\partial u] = A[\partial(A\beta)/\partial v],$$

so that the projective minimum surface is characterized by $N = 0$.

The equations of the asymptotic osculating linear complexes R_1 and R_2 of the asymptotic curves u and v at the point M are found to be

$$R_1 \equiv p_{14} - p_{23} = 0, \qquad R_2 \equiv p_{14} + p_{23} = 0$$

respectively.

Making use of the conditions of immovability, we have

$$\partial R_1/\partial v = -2(p_{12} + A^2 p_{34}), \qquad \partial R_1/\partial u = -2K p_{34},$$
$$\partial^2 R_1/\partial u\partial v = -2K(\partial \log \beta K/\partial v) p_{34} = -2(\partial A^2/\partial u) p_{34},$$
$$\partial^2 R_1/\partial u^2 = -2[B^2\gamma p_{24} - (\partial \log \gamma/\partial v) p_{12} - \gamma p_{13} + A^2(\partial \log \beta A^2/\partial v) p_{34}],$$
$$\partial^2 R_1/\partial v^2 = 2[\beta K p_{24} - (\partial K/\partial u) p_{34}].$$

2. Let C be a curve on the surface passing through the point M. At M and two consecutive points M', M'' on C there are asymptotic osculating linear complexes R_1, R_1', R_1'', which have a regulus in common. We shall call this regulus the *u-regulus of C at M*. In a similar way the v-regulus of C at M is defined. Suppose that all the u-reguli of the curves touching a given tangent t of S at M have a straight line in common, then we call this line the *u-characteristic line* of S in the direction t and we define similarly the v-characteristic line. If a u-characteristic line is also a v-characteristic line in the same tangent t, this line is then called *a characteristic line of S in the direction t.*

By hypothesis, the u-regulus of C consists of the common lines of the three linear complexes

$$R_1 = 0, \qquad dR_1 = 0, \qquad d^2R_1 = 0,$$

where d denotes the differential along C. Making use of the calculations given in **1** we may rewrite these equations in the form

$$\begin{aligned} &p_{14} - p_{23} = 0, \\ &p_{12} + [A^2 + K(du/dv)]p_{34} = 0, \\ &[B^2 - (\beta/\gamma)K(du/dv)^2]p_{24} - p_{13} + Lp_{34} = 0, \end{aligned}$$

where we have set

$$L = N/2\beta\gamma + K/\gamma\, \partial(\log \beta^3 K^2/\partial v)\, du/dv + 1/\gamma\, (\partial K/\partial u)\,(du/dv)^2 + (K/\gamma)\, d^2u/dv^2.$$

In consequence, the quadric B_1 containing the u-regulus of C is easily found to be

$$\begin{aligned} &y_1^2 - [B^2 - (\beta/\gamma)K(du/dv)^2]y_2^2 - [A^2 + K(du/dv)]y_3^2 \\ &\quad + [A^2 + K(du/dv)][B^2 - (\beta/\gamma)K(du/dv)^2]y_4^2 + L(y_1y_4 - y_2y_3) = 0, \end{aligned}$$

where y_1, y_2, y_3, y_4 denote the local coördinates of a point P with respect to the tetrahedron of Cartan, viz.,

$$P = y_1M + y_2M_1 + y_3M_2 + y_4M_3.$$

Similarly, we find the equation of the quadric B_2 which contains the v-regulus of C at M:

$$\begin{aligned} &y_1^2 - [A^2 - (\gamma/\beta)\bar{K}(dv/du)^2]y_3^2 - [B^2 + \bar{K}(dv/du)]y_2^2 \\ &\quad + [B^2 + K(dv/du)][A^2 - (\gamma/\beta)\bar{K}(dv/du)^2]y_4^2 + M(y_1y_4 - y_2y_3) = 0, \end{aligned}$$

where we have set

$$\begin{aligned} M = N/2\beta\gamma &+ \bar{K}/\beta\, \partial(\log \gamma^3\bar{K}^2/\partial u)\, dv/du \\ &+ 1/\beta\, (\partial\bar{K}/\partial v)\,(dv/du)^2 - (\bar{K}/\beta)\,(dv/du)^3(d^2u/dv^2). \end{aligned}$$

In particular *when C is an asymptotic curve v of the surface the quadric B_1 coincides with the associate quadric of Su at the given point.*

If all the asymptotic v $(u = \text{const.})$ belong to linear complexes, so that $\bar{K} = 0$, *then all the quadrics B_2 (independent of the curves C) coincide with the associate quadric, and in this case the associate quadric is stationary along any asymptotic curve v.* In fact, taking account of the equations

$$\begin{aligned} R_1 = p_{14} - p_{23} = 0, \qquad \partial R_1/\partial v = p_{12} + A^2p_{34} = 0, \\ \partial^2R_1/\partial v^2 = p_{13} - B^2p_{24} - (N/2\beta\gamma)p_{34} = 0, \end{aligned}$$

and $\bar{K} = 0$, we have

$$\partial^3 R_1/\partial v^3 = (B^2/\beta)\bar{K}p_{34} \equiv 0,$$

whence the result follows. Conversely, *if the associate quadric is stationary along any asymptotic curve v, then all the asymptotic curves v must necessarily belong to linear complexes.* This result may be demonstrated directly by means of the calculation we have so far used or derived from a theorem which we have recently established.[7] Thus a theorem of Su [8] has been improved into the following form:

If all the asymptotic curves v of a surface belong to linear complexes, then all the flecnode tangents of each curve v lie on one and the same quadric (depending upon u alone), and conversely.

In particular if the asymptotic curves of both families belong to linear complexes, all the flecnode tangents of the surface must then lie on a fixed quadric.

Let us now consider the general case. For a given tangent t and various curves touching t at M the curve of intersection of B_1 and B_2 always lies on a quadric B:

$$y_1^2 - B^2y_2^2 - A^2y_3^2 + (A^2B^2 - K\bar{K})y_4^2 + (N/2\beta\gamma + P)(y_1y_4 - y_2y_3) = 0,$$

where

$$P = (K\bar{K}dudv/(\bar{K}\gamma dv^3 + K\beta du^3)) \times [(\partial \log \beta^3K^2\bar{K}/\partial v)dv + (\partial \log \gamma^3\bar{K}^2K/\partial u)du].$$

It should be noted that the quadrics B obtained by varying t always pass through a curve given by the equations

$$\begin{cases} y_1y_4 - y_2y_3 = 0, \\ y_1^2 - B^2y_2^2 - A^2y_3^2 + (A^2B^2 - K\bar{K})y_4^2 = 0. \end{cases}$$

For each curve defined by the differential equation of the second order

$$L^2 - 4(A^2 + Kdu/dv)[B^2 - (\beta/\gamma)K(du/dv)^2] = 0,$$

the quadric B_1 decomposes into two planes. And for each curve defined by the differential equation

[7] Cf. Chenkuo Pa, "The projective theory of surfaces in ruled space," *American Journal of Mathematics*, vol. 65 (1943), pp. 712-736. See especially the last paragraph.

[8] Buchin Su, *loc. cit.*

$$L = 0,$$

the tetrahedron of Cartan at M is self-polar with respect to the corresponding quadric B_1. If a curve of one of the above classes be tangent to the curve v at M and has the contact invariant $1 - h$ (i. e. $du/dv = 0$, $d^2u/dv^2 = \gamma h$) then we have

$$(N/2\beta\gamma - Kh)^2 - 4A^2B^2 = 0,$$

or

$$(N/2\beta\gamma) - hK = 0.$$

In the case $h = 0$, surfaces of the first class have been first found by Su,[9] and those of the second class are precisely the projective minimum surfaces which may be geometrically defined by means of associate quadrics, as was shown by Su.[10]

3. If we consider all the curves on the surface touching a fixed tangent t at M, the corresponding quadrics B_1 all pass through a quadrilateral Σ_1 which may be represented by the equations:

$$\Sigma_1: \begin{array}{l} y_1y_4 - y_2y_3 = 0, \quad y_1^2 - [B^2 - (\beta/\gamma)K(du/dv)^2]y_2^2 = 0; \\ y_1y_4 - y_2y_3 = 0, \quad y_1^2 - (A^2 + Kdu/dv)y_3^2 = 0. \end{array}$$

A similar result holds for the quadrics B_2. Thus we arrive at the following

THEOREM. *At a generic point M of a surface S the u-characteristic lines (v-characteristic lines) in a given tangent direction t form a quadrilateral $\Sigma_1(\Sigma_2)$ on the quadric of Lie. For each asymptotic tangent one of these quadrilaterals decomposes into the asymptotic tangents and the other coincides with the quadrilateral of Demoulin. They coincide with each other only when t lies in one of the directions*

$$\beta K du^3 + \gamma \bar{K} dv^3 = 0$$

and then the quadric B becomes the quadric of Lie and vice versa.

For an isothermally asymptotic surface the directions just defined are those of Darboux.

For the direction $A^2dv + Kdu = 0$ two sides of Σ_1 are the asymptotic tangents of the surface at M, and the remaining sides intersect the asymptotic

---

[9] Buchin Su, *loc. cit.*

[10] Buchin Su, "Some characteristic properties of projective minimal surfaces," *Science Reports of Tôhoku Imp. Univ.* (A), vol. 24 (1936), pp. 595-600.

u-tangent. A similar result holds for the direction $B^2du + \bar{K}dv = 0$. These two directions coincide with each other when and only when the surface satisfies the relation $A^2B^2 - K\bar{K} = 0$.

4. In particular, if the curve C is taken in the asymptotic direction v so as to possess the contact invariant $1 - h$ with the asymptotic curve v at M and is denoted by C_v^h, then the quadric B_2 becomes a quadric of Darboux. The equation is easily found to be

$$y_1y_4 - y_2y_3 - (K/h)y_4^2 = 0.$$

This may be rewritten in Fubini's normal coördinates as follows:

$$xy - zt + [(\bar{K} - h(\theta_{uv} + \beta\gamma))/2h]z^2 = 0.$$

Hence we have the following theorem:

The quadric containing the v-regulus of a curve C_v^h is a Darboux quadric with index $k = \bar{K}/\beta\gamma h$. When the asymptotic curve v belongs to a linear complex, the corresponding quadric for any curve C_v^h becomes the quadric of Lie.

It seems of some interest to give here a new characteristic property of the quadric of Lie:

The two consecutive asymptotic osculating linear complexes R_1 and R'_1 (R_2 and R'_2) have always one and only one common regulus (for any curve C) on the quadric of Lie.

5. We shall conclude this paper by a remark on certain new invariant quadrics. The osculating linear complex R_2 and the two consecutive osculating linear complexes R_1 and R'_1 along a curve C have a common regulus on the quadric W_1:

$$y_1y_2 - (A^2 + Kdu/dv)y_3y_4 = 0.$$

Similarly we obtain another quadric W_2:

$$y_1y_3 - (B^2 + \bar{K}dv/du)y_2y_4 = 0.$$

For any curve C, both quadrics always pass through the two directrices of Wilczynski and two lines l_ϵ ($\epsilon = \pm 1$) given by

$$\begin{cases} \sqrt{B^2 + \bar{K}dv/du}\, y_2 - \epsilon \sqrt{A^2 + Kdu/dv}\, y_3 = 0, \\ y_1 - \epsilon \sqrt{B^2 + \bar{K}dv/du} \sqrt{A^2 + Kdu/dv}\, y_4 = 0. \end{cases}$$

The locus of the lines l_ϵ $(\epsilon = \pm 1)$ for all the curves C through M is an algebraic ruled surface of order 4:

$$(y_1y_2 - A^2y_3y_4)(y_1y_3 - B^2y_2y_4) - K\bar{K}y_2y_3y_4^2 = 0.$$

For the surface $A^2B^2 - K\bar{K} = 0$ quoted above this ruled surface decomposes into a plane and a cubic surface. In this case each of the quadrics W_1 and W_2 decomposes into planes for any curve C of the direction $A^2dv + Kdu = 0$.

THE NATIONAL UNIVERSITY OF CHEKIANG,
KWEICHOW, CHINA.

GENERALIZATION OF WARING'S PROBLEM TO ALGEBRAIC NUMBER FIELDS.*

By Carl Ludwig Siegel.

1. Introduction. Waring's problem consists in finding, for any fixed rational integer $r > 1$, a number m such that all positive rational integers ν may be decomposed into m perfect r-th powers of non-negative rational integers. The first solution was given by Hilbert.[1]

Using their powerful *circle method,* Hardy and Littlewood[2] obtained a still deeper result containing Hilbert's theorem: They proved that the number $A(\nu)$ of positive rational integral solutions λ_k $(k = 1, \cdots, m)$ of the equation

$$\lambda_1^r + \cdots + \lambda_m^r = \nu \tag{1}$$

has exactly the order of magnitude $\nu^{m/r-1}$, for any fixed $m > m_0(r)$ and $\nu \rightarrow \infty$, namely

$$A(\nu) = \frac{\Gamma^m(1 + 1/r)}{\Gamma(m/r)} \sigma \nu^{m/r-1} + o(\nu^{m/r-1}),$$

where σ, the *singular series,* is a function of ν lying between finite positive bounds.

Some years later, I[3] was interested in generalizing the circle method to an arbitrary algebraic number field K of degree n. Trying to solve the analogue of Waring's problem for K, I succeeded only in dealing with the simplest case, the decomposition into square numbers; in the case of an exponent $r > 2$, however, the generalization of the major and minor arcs of the *Farey dissection* led to a difficulty which I could not overcome at that time. Recently I found the solution.

* Received March 2, 1943.

[1] D. Hilbert, "Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem)," *Mathematische Annalen,* vol. 67 (1909), pp. 281-300.

[2] G. H. Hardy and J. E. Littlewood, "A new solution of Waring's problem," *The Quarterly Journal of Mathematics,* vol. 48 (1919), pp. 272-293; G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio Numerorum'; I: A new solution of Waring's problem," *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse,* (1920), pp. 33-54.

[3] C. L. Siegel, "Additive Zahlentheorie in Zahlkörpern," *Jahresbericht der Deutschen Mathematiker-Vereinigung,* vol. 31 (1922), pp. 22-26; C. L. Siegel, "Additive Theorie der Zahlkörper. I, II," *Mathematische Annalen,* vol. 87 (1922), pp. 1-35 and vol. 88 (1923), pp. 184-210.

Let $K^{(1)}, \cdots, K^{(n)}$ be the n conjugate fields, $K^{(l)}$ $(l = 1, \cdots, n_1)$ being real and $K^{(l)}$, $K^{(l+n_2)}$ $(l = n_1 + 1, \cdots, n_1 + n_2)$ conjugate complex, $n_1 + 2n_2 = n$. A number ν of K is called totally positive, if $\nu^{(l)} > 0$ $(l = 1, \cdots, n_1)$. Since the number of totally positive integral solutions $\lambda_1, \cdots, \lambda_m$ of (1) in K is not necessarily finite, if $n_2 > 0$, we restrict these solutions by the further conditions $|\lambda_k^{(l)}|^r < |\nu^{(l)}|$ $(k = 1, \cdots, m;$ $l = n_1 + 1, \cdots, n_1 + n_2)$ and denote their number by $A(\nu)$.

In the case of the field of rational numbers, it is trivial that any positive integer ν is a sum of r-th powers of integers, namely ν times 1^r. It is easily seen that the corresponding statement, without further restriction, does not hold for an arbitrary K: In a real quadratic field with discriminant $4d$, $d \equiv 2, 3 \pmod 4$, all integral squares have the form $(a + b\sqrt{d})^2 = a^2 + b^2 d + 2ab\sqrt{d}$ with rational integral a, b; consequently a number $p + q\sqrt{d}$ with rational integral p, q and odd q is never a sum of integral squares. This example leads to the introduction of the ring J_r generated by the r-th powers of all integers in K; it consists of all numbers $a_1\lambda_1^r + \cdots + a_h\lambda_h^r$ $(h = 1, 2, \cdots)$, where $\lambda_1, \cdots, \lambda_h$ are integers in K and $a_1, \cdots, a_h$ are rational integers. Obviously $A(\nu) = 0$, if ν is not a number of J_r. It will be proved that J_r is an *order*, and an explicit construction of J_r will be given. In the above example, J_2 consists of all numbers $p + q\sqrt{d}$ with even q.

Let D be the absolute value of the discriminant of K, and denote by $N(\nu) = M$ the norm of the totally positive integer ν in K.

THEOREM. *For any fixed*

$$m > (2^{r-1} + n)nr \tag{2}$$

and $M \to \infty$

$$A(\nu) = D^{(1-m)/2}\sigma_0\sigma M^{m/r-1} + o(M^{m/r-1}), \tag{3}$$

where σ_0 *is a positive number depending only upon* n_1, n_2, m, r *and, in particular,*

$$\sigma_0 = \left(\frac{\Gamma^m(1 + 1/r)}{\Gamma(m/r)}\right)^n \qquad (n_2 = 0). \tag{4}$$

The singular series σ *lies between finite positive bounds, whenever* ν *belongs to* J_r, *and* $\sigma = 0$ *otherwise.*

As a consequence of this Theorem, all totally positive numbers of J_r with sufficiently large norm are sums of a bounded number of r-th powers of totally positive integers in K. It might be suggested, in analogy to the case $n = 1$, that then all totally positive numbers of J_r will be such sums; however, the

following example shows that this is not true without further restriction. In the quadratic field with discriminant 24, the totally positive number $5+2\sqrt{6}$ of J_2 cannot be expressed as a sum of integral squares. On the other hand, it can be proved that all totally positive numbers of J_r are a sum of a bounded number of integral r-th powers, if the field K is not totally real; but this condition is not necessary.

For the sake of brevity, the proof of the Theorem will be given only in the case of a totally real field K, i. e., $n_2=0$; as a matter of fact, the proof in the general case proceeds on the same lines, the formulae being somewhat more cumbersome. Probably, the reader will also notice several possible generalizations of the Theorem. The proof uses Vinogradow's idea of substituting finite trigonometrical sums for the generating power series in the original method of Hardy and Littlewood, with some modifications due to Landau.[4] For $n=1$, the domains B_γ introduced in Section **2** are the major arcs in the definition of Weyl.[5]

Following Dedekind, we abbreviate the function $e^{2\pi ix}$ by the symbol 1^x. Henceforth, small Greek letters without upper index denote points in the real n-dimensional euclidean space R, the coördinates being designated by upper indices; e. g., $\xi=\{\xi^{(1)},\cdots,\xi^{(n)}\}$. The numbers α of the totally real field K are represented by the points $\alpha=\{\alpha^{(1)},\cdots,\alpha^{(n)}\}$ of R, where $\alpha^{(l)}$ is the conjugate of α in $K^{(l)}$ $(l=1,\cdots,n)$. We define $S(\xi)=\xi^{(1)}+\cdots+\xi^{(n)}$, $N(\xi)=\xi^{(1)}\cdots\xi^{(n)}$. A relationship involving small Greek letters without upper index, the symbols S and N excepted, stands always as an abbreviation of the n corresponding relationships for the coördinates; e. g., the inequality $\alpha<\xi$ means $\alpha^{(l)}<\xi^{(l)}$ $(l=1,\cdots,n)$.

Small German letters denote ideals in K. The symbols $N(\mathfrak{a})$, $\mathfrak{a}\,|\,\alpha$, $(\mathfrak{a},\mathfrak{b})$ have their usual meaning. The numbers of any ideal $\mathfrak{a}$ constitute a lattice in R and any basis of $\mathfrak{a}$ defines a fundamental parallelepiped in this lattice with the volume $D^{\frac{1}{2}}N(\mathfrak{a})$. We choose a basis $\omega_1,\cdots,\omega_n$ of the unit ideal; then the inverse matrix $(\omega_k^{(l)})^{-1}=(\rho_l^{(k)})$ defines a basis $\rho_1,\cdots,\rho_n$ of $\mathfrak{d}^{-1}$, where $\mathfrak{d}$ is the ramification ideal of K and $N(\mathfrak{d})=D$; let E be the corresponding parallelepiped in R, with the volume $D^{-\frac{1}{2}}$.

For any totally positive unit ϵ in K, the formula $A(\epsilon^r\nu)=A(\nu)$ holds good. Since there exist $n-1$ independent units in K, we may assume, during the proof of the Theorem, that

---

[4] E. Landau, "Über die neue Winogradoffsche Behandlung des Waringschen Problems," *Mathematische Zeitschrift*, vol. 31 (1930), pp. 319-338.

[5] H. Weyl, "Bemerkung über die Hardy-Littlewoodschen Untersuchungen zum Waringschen Problem," *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse*, (1921), pp. 189-192.

(5) $$\nu = O(M^{1/n}), \qquad \nu^{-1} = O(M^{-(1/n)}).$$

We introduce the abbreviations

$$a = 1/nr - 2^{r-1}/(m-1), \quad h = M^{(1/n)(1+a-1/r)}, \quad t = M^{(1/n)(1/r-a)};$$

by (2), the constant a is positive. The symbols O and o refer always to the passage to the limit $M \to \infty$.

Define

(6) $$f(\xi) = \sum_{0<\lambda<\nu^{1/r}} 1^{S(\lambda^r \xi)},$$

where λ runs over all integers in K satisfying $0 < \lambda < \nu^{1/r}$, and

(7) $$g(\xi) = f^m(\xi) 1^{-S(\nu\epsilon)}.$$

Since $S(\beta)$ is a rational integer for all numbers β in $\mathfrak{d}^{-1}$, we have

(8) $$A(\nu) = D^{\frac{1}{2}} \int_E g(\xi) dv,$$

where $dv = d\xi^{(1)} \cdots d\xi^{(n)}$ is the volume element in R.

2. Generalized Farey dissection. For any number γ of K, let $\mathfrak{a} = \mathfrak{a}_\gamma$ be the denominator of $\gamma\mathfrak{d}$, i.e., $\mathfrak{a} = (1, \gamma\mathfrak{d})^{-1}$. We define B_γ to be the set of all points ξ of R fulfilling the condition

(9) $$N(\operatorname{Max}(h \mid \xi - \gamma \mid, t^{-1})) \leq N(\mathfrak{a}^{-1}).$$

It is clear that B_γ is vacuous in case $N(\mathfrak{a}) > t^n = M^{1/r-a}$.

In the following, it will be sometimes tacitly assumed that M is sufficiently large, i.e., $M > M_0$, where M_0 depends only upon K, m, r.

LEMMA 1. *If $\gamma \neq \hat{\gamma}$, then B_γ and $B_{\hat{\gamma}}$ have no common point.*

Proof. Let ξ be a common point of B_γ and $B_{\hat{\gamma}}$, and put

$$\operatorname{Max}(h \mid \xi - \gamma \mid, t^{-1}) = \tau^{-1}, \quad \operatorname{Max}(h \mid \xi - \hat{\gamma} \mid, t^{-1}) = \hat{\tau}^{-1}, \quad \mathfrak{a}_{\hat{\gamma}} = \hat{\mathfrak{a}};$$

then

$$\tau \leq t, \quad \hat{\tau} \leq t, \quad N(\mathfrak{a}\hat{\mathfrak{a}}) \leq N(\tau\hat{\tau})$$
$$|\gamma - \hat{\gamma}| \leq |\xi - \gamma| + |\xi - \hat{\gamma}| \leq h^{-1}(\tau^{-1} + \hat{\tau}^{-1}) \leq 2t(h\tau\hat{\tau})^{-1}$$
$$N((\gamma - \hat{\gamma})\mathfrak{a}\hat{\mathfrak{a}}) \leq (2th^{-1})^n = 2^n M^{2/r-1-2a} = o(1).$$

On the other hand, the ideal $(\gamma - \hat{\gamma})\mathfrak{a}\hat{\mathfrak{a}}\mathfrak{d}$ is integral and therefore

$$N((\gamma - \hat{\gamma})\mathfrak{a}\hat{\mathfrak{a}}) \geq D^{-1};$$

this is a contradiction.

LEMMA 2. *Let ξ be a point not lying in any B_γ. There exist an integer α in K and a number β of $\mathfrak{d}^{-1}$ such that*

$$|\alpha\xi - \beta| < h^{-1}, \quad 0 < |\alpha| \leq h, \tag{10}$$

$$\operatorname{Max}(h\,|\alpha\xi - \beta|, |\alpha|) \geq D^{-\frac{1}{2}}, \tag{11}$$

$$\operatorname{Max}(|\alpha^{(1)}|, \cdots, |\alpha^{(n)}|) > t, \tag{12}$$

$$N((\alpha, \beta\mathfrak{d})) \leq D^{\frac{1}{2}}. \tag{13}$$

Proof. Applying Minkowski's theorem to the system of $2n$ linear forms

$$\sum_{l=1}^{n} \omega_l^{(k)} x_l, \qquad \sum_{l=1}^{n} (\xi^{(k)} \omega_l^{(k)} x_l - \rho_l^{(k)} y_l) \qquad (k = 1, \cdots, n)$$

with determinant ± 1, we obtain a solution α, β of (10) with $1\,|\,\alpha$, $\mathfrak{d}^{-1}\,|\,\beta$. Set $\alpha^{-1}\beta = \gamma$ and $(1, \gamma\mathfrak{d})^{-1} = \mathfrak{a}$; then $\mathfrak{a}\,|\,\alpha$, $N(\mathfrak{a}) \leqq |N(\alpha)|$. Since ξ is not a point of B_γ, we have

$$N(\operatorname{Max}(h\,|\xi - \gamma|, t^{-1}) > N(\mathfrak{a}^{-1}), \qquad N(\operatorname{Max}(1, t^{-1}\,|\alpha|)) > 1,$$

and (12) follows.

Consider now all pairs α, β satsifying the conditions $1\,|\,\alpha$, $\mathfrak{d}^{-1}\,|\,\beta$ and (10); they form a finite set $\mathfrak{S}$. Choose α, β in $\mathfrak{S}$ such that the number $\operatorname{Max}(|\alpha^{(1)}|, \cdots, |\alpha^{(n)}|)$ attains its minimum b; by (12), $b > t$. We are going to demonstrate that this pair fulfills also the conditions (11) and (13). Put $(\alpha, \beta\mathfrak{d})^{-1} = \mathfrak{q}$ and let κ be a number of $\mathfrak{q}$. The pair $\kappa\alpha = \hat{\alpha}$, $\kappa\beta = \hat{\beta}$ belongs to $\mathfrak{S}$, whenever the conditions

$$|\kappa|\,|\alpha\xi - \beta| < h^{-1}, \qquad 0 < |\kappa|\,|\alpha| \leq h \tag{14}$$

are satisfied, and then, by the definition of b,

$$\operatorname{Max}(|\hat{\alpha}^{(1)}|, \cdots, |\hat{\alpha}^{(n)}|) \geq b. \tag{15}$$

If $N(\mathfrak{q}) < D^{-\frac{1}{2}}$, Minkowski's theorem shows the existence of a number κ in $\mathfrak{q}$ such that $0 < |\kappa| < 1$. Then (14) is satisfied, by (10), and (15) leads to a contradiction, since $|\hat{\alpha}| < |\alpha|$. Consequently $N(\mathfrak{q}^{-1}) \leq D^{\frac{1}{2}}$, and this is the assertion (13).

In order to prove also (11), we may obviously assume

$$|\alpha^{(1)}| < D^{-\frac{1}{2}}, \tag{16}$$

whence $n > 1$. Applying again Minkowski's theorem, we construct a number κ in $\mathfrak{q}$ with

$$(17) \qquad 0 < |\kappa^{(1)}| \leq D^{\frac{1}{2}}, \qquad |\kappa^{(l)}| < 1 \qquad (l = 2, \cdots, n);$$

then $|\hat{\alpha}^{(1)}| < 1$ and $|\hat{\alpha}^{(l)}| < |\alpha^{(l)}|$ $(l = 2, \cdots, n)$. Since $|\alpha^{(l)}| = b > t$ for at least one value of l, we have

$$\operatorname{Max}(|\hat{\alpha}^{(1)}|, \cdots, |\hat{\alpha}^{(n)}|) < \operatorname{Max}(1, |\alpha^{(2)}|, \cdots, |\alpha^{(n)}|) = b;$$

in contradiction to (15), if the pair $\hat{\alpha}, \hat{\beta}$ were in $\mathfrak{S}$; consequently the conditions (14) are not all satisfied. On the other hand, by (10), (16), (17),

$$0 < |\kappa|\, |\alpha| \leq h, \quad |\kappa^{(l)}|\, |\alpha^{(l)}\xi^{(l)} - \beta^{(l)}| < h^{-1} \qquad (l = 2, \cdots, n);$$

hence

$$|\alpha^{(1)}\xi^{(1)} - \beta^{(1)}| \geq (h\, |\kappa^{(1)}|)^{-1} \geq D^{-\frac{1}{2}} h^{-1},$$

and (11) is proved.

Let γ run over all numbers of K. It follows from (9) that only a finite number of the domains B_γ enter into the fundamental parallelepiped E; let E_0 be the set of all points of E not contained in any B_γ. We choose now a complete system Γ of modulo $\mathfrak{d}^{-1}$ incongruent numbers γ with $N(\mathfrak{a}_\gamma) \leqq t^n$. If ξ is a point of $E - E_0$, then there exist a number β in $\mathfrak{d}^{-1}$ and a number γ in Γ such that $\xi - \beta = \eta$ lies in B_γ; in view of Lemma 1, β and γ are uniquely determined. On the other hand, for any η in R, there exists a number β in $\mathfrak{d}^{-1}$ such that $\eta + \beta = \xi$ lies in E, and β is uniquely determined except when ξ lies on the frontier of E. Consequently, the formula

$$(18) \qquad \int_E g(\xi)\,dv = \int_{E_0} g(\xi)\,dv + \sum_{\gamma \subset \Gamma} \int_{B_\gamma} g(\xi)\,dv$$

holds for an integrable function $g(\xi)$, whenever $g(\xi + \beta) = g(\xi)$ for all β in $\mathfrak{d}^{-1}$, and in particular for the function defined in (7).

3. Approximation to $f(\xi)$ on B_γ. Let ξ be a point of B_γ, $\xi - \gamma = \zeta$ and $\mathfrak{a} = (1, \gamma\mathfrak{d})^{-1}$; then

$$N(\operatorname{Max}(h\,|\zeta|, t^{-1})) \leq N(\mathfrak{a}^{-1}), \qquad N(\mathfrak{a}) \leq M^{1/r-a}.$$

We determine a point $\theta > 0$ such that

$$\theta \operatorname{Max}(h\,|\zeta|, t^{-1}) \leqq D^{1/2n}, \qquad N(\theta) = D^{1/2} N(\mathfrak{a}).$$

On account of Minkowski's theorem, the ideal $\mathfrak{a}$ contains a number α with $0 < |\alpha| \leq \theta$. Then $\alpha\mathfrak{a}^{-1} = \mathfrak{b}$ is an integral ideal and $N(\mathfrak{b}) \leq D^{\frac{1}{2}}$; hence $\mathfrak{b}$

belongs to a finite set depending only upon K. Choose a basis $\beta_1, \cdots, \beta_n$ of $\mathfrak{b}^{-1}$; then $\mathfrak{a} = \alpha\mathfrak{b}^{-1}$ has the basis $\alpha_k = \alpha\beta_k$ $(k = 1, \cdots, n)$ and

$$\alpha_k = O(\theta) \qquad (k = 1, \cdots, n).$$

If μ runs over a complete system of residues modulo $\mathfrak{a}$, we have, by (6)

$$f(\xi) = \sum_{\mu \pmod{\mathfrak{a}}} 1^{S(\mu^r\gamma)} \sum_{\substack{0 < \lambda+\mu < \nu^{1/r} \\ \mathfrak{a}|\lambda}} 1^{S((\lambda+\mu)^r\zeta)}. \tag{19}$$

Put $\lambda = g_1\alpha_1 + \cdots + g_n\alpha_n$, with rational integral $g_1, \cdots, g_n$, and let E_λ be the parallelepiped of the points $\eta = y_1\alpha_1 + \cdots + y_n\alpha_n$ with $g_k \leq y_k \leq g_k + 1$ $(k = 1, \cdots, n)$. For all λ occurring in (19),

$$\eta - \lambda = O(\theta) = O(t) = o(\nu^{1/r})$$
$$(\eta + \mu)^r\zeta - (\lambda + \mu)^r\zeta = (\eta - \lambda)\zeta O(|\eta + \mu|^{r-1} + |\lambda + \mu|^{r-1})$$
$$= \zeta\theta O(\nu^{1-1/r}) = h^{-1}O(\nu^{1-1/r}) = O(M^{-a/n}).$$

Since E_λ has the volume $D^{\frac{1}{2}}N(\mathfrak{a})$, we obtain

$$1^{S((\lambda+\mu)^r\zeta)} = D^{-\frac{1}{2}}N(\mathfrak{a}^{-1}) \int_{E_\lambda} 1^{S((\eta+\mu)^r\zeta)} dv + O(M^{-a/n}). \tag{20}$$

The number of all λ in $\mathfrak{a}$, satisfying $0 < \lambda + \mu < \nu^{1/r}$ for fixed μ, is less than

$$1 + N(\nu^{1/r})N(\mathfrak{a}^{-1}) = N(\mathfrak{a}^{-1})O(M^{1/r}). \tag{21}$$

On the other hand, for fixed μ, the sum of the E_λ is contained in the rectangular parallelepiped $-c\theta < \eta + \mu < \nu^{1/r} + c\theta$ and contains the smaller parallelepiped $c\theta < \eta + \mu < \nu^{1/r} - c\theta$, with a suitably chosen positive $c = O(1)$. Since the difference of the volumes of these two parallelepipeds is $M^{(1/r)(1-1/n)}O(t) = O(M^{1/r-a/n})$, we obtain, by (20) and (21),

$$\sum_{\substack{0 < \lambda+\mu < \nu^{1/r} \\ \mathfrak{a}|\lambda}} 1^{S((\lambda+\mu)^r\zeta)} = D^{-\frac{1}{2}}N(\mathfrak{a}^{-1}) \int_{0 < \eta < \nu^{1/r}} 1^{S(\eta^r\zeta)} dv + N(\mathfrak{a}^{-1})O(M^{1/r-a/n}).$$

Setting

$$N(\mathfrak{a}^{-1}) \sum_{\mu \pmod{\mathfrak{a}}} 1^{S(\mu^r\gamma)} = G(\gamma),$$

we get the required approximation

$$f(\xi) = D^{-\frac{1}{2}}G(\gamma)N\left(\int_0^{\nu^{1/r}} 1^{\eta^r\zeta} d\eta\right) + O(M^{1/r-a/n}). \tag{22}$$

4. Estimation of $f(\xi)$ on E_0. Let ξ be a point of E_0. Applying Weyl's method of estimating trigonometrical sums, we obtain

$$(23) \qquad |f(\xi)|^{2^{r-1}} = O(M^{(1/r)2^{r-1}-1}) \sum_{\lambda_1,\ldots,\lambda_{r-1}} |\sum_{\lambda} 1^{r!\,S(\lambda\lambda_1\ldots\lambda_{r-1}\xi)}|,$$

where the summation is carried over the systems of integers $\lambda, \lambda_1, \cdots, \lambda_{r-1}$ in K defined by the $2^{r-1}n$ conditions

$$0 < \lambda + \lambda_{k_1} + \cdots + \lambda_{k_g} < \nu^{1/r}$$
$$(1 \leq k_1 < k_2 < \cdots < k_g \leq r-1;\ g = 0, 1, \cdots, r-1).$$

Then

$$-\nu^{1/r} < \lambda_k < \nu^{1/r} \qquad (k = 1, \cdots, r-1),$$

and for each system $\lambda_1, \cdots, \lambda_{r-1}$ the point λ runs over all integers in a rectangular parallelepiped $P = P(\lambda_1, \cdots, \lambda_{r-1})$ whose sides are $< \nu^{1/r} = O(M^{1/nr})$.

Put

$$(24) \qquad r!\,\lambda_1 \cdots \lambda_{r-1} = \mu,$$
$$\sum_{\lambda \subset P} 1^{S(\lambda\mu\xi)} = u = u(\lambda_1, \cdots, \lambda_{r-1}).$$

For any fixed integer ω in K, we obtain

$$u 1^{S(\omega\mu\xi)} = \sum_{\lambda-\omega \subset P} 1^{S(\lambda\mu\xi)} = u + O(M^{(1/r)(1-1/n)}),$$

whence

$$(25) \quad u = O(M^{(1/r)(1-1/n)}) \operatorname{Min}(M^{1/nr}, |1^{S(\omega_1\mu\xi)} - 1|^{-1}, \cdots, |1^{S(\omega_n\mu\xi)} - 1|^{-1}),$$

where $\omega_1, \cdots, \omega_n$ are the basis of all integers in K.

Let

$$S(\omega_k\mu\xi) = a_k + d_k, \qquad -\tfrac{1}{2} \leq d_k < \tfrac{1}{2} \qquad (k = 1, \cdots, n),$$

with rational integral a_k, and define

$$\sum_{k=1}^{n} a_k\rho_k = \vartheta, \qquad \sum_{k=1}^{n} d_k\rho_k = \zeta;$$

then

$$\mathfrak{d}^{-1} | \vartheta, \quad \mu\xi = \vartheta + \zeta, \quad d_k = S(\omega_k\zeta), \quad 1^{S(\omega_k\mu\xi)} = 1^{d_k} \quad (k = 1, \cdots, n).$$

In view of Lemma 2, there exist two numbers α, β in K satisfying (10), (11), (12), (13) and $1 | \alpha$, $\mathfrak{d}^{-1} | \beta$. If exactly q of the conjugates $\alpha^{(1)}, \cdots, \alpha^{(n)}$ are of absolute value $< D^{-\frac{1}{2}}$, then $0 \leq q \leq n-1$, by (12), and we may assume

(26) $|\alpha^{(n)}| > t,\ |\alpha^{(k)}| < D^{-\frac{1}{2}}\ (1 \leq k \leq q),\ |\alpha^{(k)}| \geq D^{-\frac{1}{2}}\ (q+1 \leq k \leq n).$

Since $\zeta = O(1)\operatorname{Max}(|d_1|, \cdots, |d_n|)$, we conclude from (25) that

(27) $$u(\lambda_1, \cdots, \lambda_{r-1}) = O(M^{(1/r)(1-1/n)}) \operatorname{Min}(M^{1/nr}, |\zeta^{(n)}|^{-1}).$$

The point ζ depends only upon μ, for any given ξ in E_0. On the other hand, for fixed μ, the number of integral solutions $\lambda_1, \cdots, \lambda_{r-1}$ of (24), satisfying $|\lambda_k| < \nu^{1/r}$ $(k = 1, \cdots, r-1)$, is $O(M^{1-2/r})$ in case $\mu = 0$ and $O(M^{\Delta})$ otherwise, Δ denoting an arbitrarily small positive number. Introduce the abbreviation

(28) $$\operatorname{Min}(M^{1/nr}, |\zeta^{(n)}|^{-1}) = j(\mu);$$

then, by (23) and (27),

(29) $$|f(\xi)|^{2^{r-1}} = O(M^{(1/r)(2^{r-1}-1)}) + O(M^{\Delta+(1/r)(2^{r-1}+1-1/n)-1}) \sum_{|\mu| < r!\,\nu^{1-1/r}} j(\mu),$$

where μ runs over all integers in K satisfying

(30) $$|\mu| < r!\,\nu^{1-1/r}.$$

Let $g_1, \cdots, g_n$ be rational integers and let $W = W(g_1, \cdots, g_n) > 0$ be the number of different integers μ in K fulfilling (30) and the n conditions

(31) $$g_k \leq 2D^{1/n}\zeta^{(k)} \operatorname{Max}(|\alpha^{(k)}|, D^{-\frac{1}{2}}) < g_k + 1 \qquad (k = 1, \cdots, n).$$

Let $\hat{\mu}$ be one of these μ and $\hat{\mu}\xi = \hat{\vartheta} + \hat{\zeta}$. Setting $\alpha\xi - \beta = \delta$ and $\alpha(\vartheta - \hat{\vartheta}) - \beta(\mu - \hat{\mu}) = \kappa$, we obtain

(32) $$|\alpha(\zeta - \hat{\zeta})| < \tfrac{1}{2}D^{-(1/n)},$$

(33) $$\kappa = \delta(\mu - \hat{\mu}) - \alpha(\zeta - \hat{\zeta}).$$

On account of (10) and (30),

$$\delta(\mu - \hat{\mu}) = h^{-1}O(M^{(1/n)(1-1/r)}) = O(M^{-(a/n)}) = o(1),$$

whence, by (32) and (33), $|\kappa| < D^{-(1/n)}$; but κ is a number of $\mathfrak{d}^{-1}$, and consequently $\kappa = 0$,

(34) $$(\mu - \hat{\mu})/\alpha = (\vartheta - \hat{\vartheta})/\beta = (\zeta - \hat{\zeta})/\delta.$$

This proves that α is a divisor of $(\mu - \hat{\mu})\beta\mathfrak{d}$. In view of (13), we infer that $\alpha | v(\mu - \hat{\mu})$, where v denotes a positive rational integer depending only upon K. Since

$$(\mu - \hat{\mu})/\alpha = \alpha^{-1}O(M^{(1/n)(1-1/r)})$$

and, by (11), (26), (34),

$$(\mu^{(k)}-\hat{\mu}^{(k)})/\alpha^{(k)}=(\zeta^{(k)}-\hat{\zeta}^{(k)})/\delta^{(k)}=O(h) \qquad (1\leq k\leq q),$$

it follows that the number of values of the differences $\mu-\hat{\mu}$ is

$$1+O(h^q)\prod_{k=q+1}^{n}(M^{(1/n)(1-1/r)}\mid\alpha^{(k)}\mid^{-1});$$

hence

$$W=1+O(M^{1-1/r+a(1-1/n)})\prod_{k=q+1}^{n}\mid\alpha^{(k)}\mid^{-1}.$$

In view of $\zeta=O(1)$, we have $g_k=O(1)\,(k\leqq q)$ and $g_k=O(\mid\alpha^{(k)}\mid)$ $(k>q)$, by (26) and (31). For any fixed $g_n=g$, the number of possible systems $g_1,\cdots,g_{n-1}$ in (31), with $W>0$, is $O(\prod_{k=q+1}^{n-1}\mid\alpha^{(k)}\mid)$. Consequently, the number of integral μ in K, fulfilling (30) and the single condition

$$g\leqq 2D^{1/n}\mid\alpha^{(n)}\mid\zeta^{(n)}<g+1, \tag{35}$$

is

$$\begin{aligned}W_g&=\sum_{g_1,\cdots,g_{n-1}}W(g_1,\cdots,g_{n-1},g)\\&=O(1+M^{1-1/r+a(1-1/n)}\prod_{k=q+1}^{n}\mid\alpha^{(k)}\mid^{-1})\prod_{k=q+1}^{n-1}\mid\alpha^{(k)}\mid\\&=O(h^{n-q-1}+M^{1-1/r+a(1-1/n)}\mid\alpha^{(n)}\mid^{-1})\\&=M^{(1-1/n)(1-1/r+a)}O(1+M^{(1/n)(1-1/r)}\mid\alpha^{(n)}\mid^{-1}).\end{aligned} \tag{36}$$

Defining

$$\sum_{0\leqq g<|\alpha^{(n)}|}\operatorname{Min}(M^{1/nr},g^{-1}\mid\alpha^{(n)}\mid)=Q$$

we obtain, by (28), (35) and (36),

$$\begin{aligned}\sum_{|\mu|<r!\,\nu^{1-1/r}}j(\mu)&=\sum_g W_gO(\operatorname{Min}(M^{1/nr},\mid g\mid^{-1}\mid\alpha^{(n)}\mid,\mid g+1\mid^{-1}\mid\alpha^{(n)}\mid)\\&=M^{(1-1/n)(1-1/r+a)}QO(1+M^{(1/n)(1-1/r)}\mid\alpha^{(n)}\mid^{-1}).\end{aligned} \tag{37}$$

By (10) and (26),

$$Q=O(M^{1/nr}+\mid\alpha^{(n)}\mid\log\mid\alpha^{(n)}\mid)=O(M^{1/nr}+h\log h)=O(M^{(1/n)(1-1/r+a)}\log M)$$
$$QM^{(1/n)(1-1/r)}\mid\alpha^{(n)}\mid^{-1}=(t^{-1}+M^{-(1/nr)}\log h)O(M^{1/n})=O(M^{(1/n)(1-1/r+a)}\log M),$$

and (29), (37) lead to the required estimate

$$\begin{aligned}\mid f(\xi)\mid^{2^{r-1}}&=O(M^{\Delta+(1/r)2^{r-1}+a-1/nr})=O(M^{\Delta+(1/r-1/(m-1))2^{r-1}}),\\f(\xi)&=o(M^{1/r-1/m}).\end{aligned} \tag{38}$$

5. Proof of the asymptotic formula for $A(\nu)$. The relationship

$$G(\gamma) = N(\mathfrak{a}^{-1}) \sum_{\mu \pmod{\mathfrak{a}}} 1^{S(\mu^r \gamma)} = (N(\mathfrak{a}))^{-(1/r)} O(1) \tag{39}$$

may be proved in exactly the same way as in the case $n = 1$. Moreover

$$\int_0^{\nu^{1/r}} 1^{\eta^r \zeta} d\eta = O(\mathrm{Min}(\nu^{1/r}, |\zeta|^{-(1/r)}));$$

consequently (22) leads to the formula

$$f^m(\xi) = D^{-(m/2)} G^m(\gamma) N^m\Big(\int_0^{\nu^{1/r}} 1^{\eta^r \zeta} d\eta\Big) + O(M^{m(1/r-a/n)})$$
$$+ (N(\mathfrak{a}))^{-(m-1)/r} N(\mathrm{Min}(\nu^{(m-1)/r}, |\zeta|^{-(m-1)/r})) O(M^{1/r-a/n}),$$

for all $\xi = \gamma + \zeta$ in B_γ, whence

$$\sum_{\gamma \subset \Gamma} \int_{B_\gamma} g(\xi)\, dv = D^{-(m/2)} \sum_{\gamma \subset \Gamma} G^m(\gamma) 1^{-S(\nu\gamma)} \int_{B_\gamma} N^m\Big(\int_0^{\nu^{1/r}} 1^{\eta^r \zeta} d\eta\Big) 1^{-S(\nu\zeta)} dv$$
$$+ O(M^{m(1/r-a/n)}) + O(M^{m/r-a/n-1}).$$

On the other hand, for any point ξ of $R - B_\gamma$, the inequality

$$h\, |\zeta^{(k)}| > (N(\mathfrak{a}))^{-1/n}$$

is true for at least one k; therefore

$$\int_{R-B_\gamma} N^m\Big(\int_0^{\nu^{1/r}} 1^{\eta^r \zeta} d\eta\Big) 1^{-S(\nu\zeta)} dv = \int_{R-B_\gamma} N^m(\mathrm{Min}(\nu^{1/r}, |\zeta|^{-1/r}))\, dv\, O(1)$$
$$= \int_{h^{-1}(N(\mathfrak{a}))^{-(1/n)}}^{\infty} z^{-(m/r)} dz\, O(M^{(m/r-1)(1-1/n)}) = (N(\mathfrak{a}))^{(1/n)(m/r-1)} O(M^{(m/r-1)(1+a/n-1/nr)}).$$

Since

$$\int_R N^m\Big(\int_0^{\nu^{1/r}} 1^{\xi\eta^r} d\eta\Big)\, 1^{-S(\nu\xi)} dv = \sigma_0 M^{m/r-1},$$

with the constant σ_0 defined in (4), and $ma > (m-1)a = (m-1)/nr - 2^{r-1} \geqq n$, by (3), we obtain

$$\sum_{\gamma \subset \Gamma} \int_{B_\gamma} g(\xi)\, dv - D^{-(m/2)} \sigma_0 \sigma M^{m/r-1} \tag{40}$$
$$= o(M^{m/r-1}) + O(M^{(m/r-1)(1+a/n-1/nr)}) \sum_{\gamma \subset \Gamma} N(\mathfrak{a}^{-1})$$
$$= o(M^{m/r-1}) + O(M^{m/r-1-(1/n)(1/r-a)(m/r-n-1)}) = o(M^{m/r-1}),$$

with

$$\sigma = \sum_{\gamma (\mathrm{mod}\, \mathfrak{d}^{-1})} G^m(\gamma) 1^{-S(\nu\gamma)},$$

where γ runs over a complete system of incongruent numbers in K modulo $\mathfrak{d}^{-1}$. The first assertion of the Theorem, namely formula (3), follows now from (8), (18), (38) and (40).

6. The singular series. For every ideal $\mathfrak{a}$ in K we define

$$H(\mathfrak{a}) = \sum_{\gamma} G^m(\gamma) 1^{-S(\nu\gamma)},$$

where γ runs over a complete system of modulo $(\mathfrak{a}\mathfrak{d})^{-1}$ incongruent numbers satisfying $(1, \gamma\mathfrak{d})^{-1} = \mathfrak{a}$; then

$$\sigma = \sum_{\mathfrak{a}} H(\mathfrak{a}),$$

the summation extended over all integral ideals $\mathfrak{a}$.

Denote by $A(\nu, \mathfrak{a})$ the number of modulo $\mathfrak{a}$ incongruent systems of integral solutions $\lambda_1, \cdots, \lambda_m$ of the congruence

$$\lambda_1{}^r + \cdots + \lambda_m{}^r \equiv \nu \; (\mathrm{mod}\; \mathfrak{a}),$$

and let $A_0(\nu, \mathfrak{a})$ be the number of modulo $\mathfrak{a}$ primitive solutions, i. e., satisfying $(\lambda_1, \cdots, \lambda_m, \mathfrak{a}) = 1$.

Exactly as in the known case $n = 1$, the following four statements are proved, for any $m > 2r$. The singular series σ has the factorization

$$\sigma = \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}, \qquad \sigma_{\mathfrak{p}} = \sum_{q=0}^{\infty} H(\mathfrak{p}^q),$$

where $\mathfrak{p}$ runs over all prime ideals in K; the singular series vanishes, if and only if $\sigma_{\mathfrak{p}} = 0$ for at least one $\mathfrak{p}$; let $\mathfrak{p}^b$ and $\mathfrak{p}^c$ denote the highest powers of $\mathfrak{p}$ dividing ν and r, then

$$\sigma_{\mathfrak{p}} = A(\nu, \mathfrak{p}^q) N(\mathfrak{p}^{-(m-1)q}) \quad (q > b + 2c), \quad \sigma_{\mathfrak{p}} \geqq A_0(\nu, \mathfrak{p}^q) N(\mathfrak{p}^{-(m-1)q}) \quad (q > 2c);$$

the singular series possesses a positive lower bound for all ν in J_r, if $A_0(\nu, \mathfrak{p}^{2c+1}) > 0$ for all prime ideals $\mathfrak{p}$.

In order to prove the second assertion of the Theorem, concerning the value of σ, we consider now more closely the ring J_r, generated by the r-th powers of all integers in K. On account of the identity

$$\sum_{k=0}^{r-1} (-1)^{r-k-1} \binom{r-1}{k} \{(x+k)^r - k^r\} = r!\,x,$$

the number $r!\,\mu$ belongs to J_r, for any integer μ in K; since also 1 belongs to J_r, the ring J_r is an order. Let $\mathfrak{p}$ be a prime ideal; we say that an integer ν of K belongs to $J_r(\mathfrak{p})$, whenever ν is congruent, modulo $\mathfrak{p}^q$, to a number ν_q of J_r, for $q = 1, 2, \cdots$; obviously $J_r(\mathfrak{p})$ contains J_r and constitutes also an order. If $(r!, \mathfrak{p}) = 1$, then $J_r(\mathfrak{p}) = J_r$. Moreover, it is easily seen that ν belongs to $J_r(\mathfrak{p})$, if the congruence $\nu \equiv \nu_q \pmod{\mathfrak{p}^q}$ has a solution ν_q in J_r for the fixed exponent $q = 2c + 1$, with the above definition of c; consequently ν belongs to $J_r(\mathfrak{p})$, if and only if the congruence

$$x_1\eta_1{}^r + \cdots + x_h\eta_h{}^r \equiv \nu \pmod{\mathfrak{p}^{2c+1}}$$

has a solution in non-negative rational integers $x_k < h$ $(k = 1, \cdots, h)$, where $h = N(\mathfrak{p}^{2c+1})$ and $\eta_1, \cdots, \eta_h$ constitute a complete system of integral residues modulo $\mathfrak{p}^{2c+1}$ in K. On the other hand, using a basis of the order J_r, one proves immediately that ν belongs again to J_r, if it belongs to $J_r(\mathfrak{p})$ for all $\mathfrak{p}$. These remarks provide a method for the explicit construction of J_r.

If ν is not in J_r, then it is not in $J_r(\mathfrak{p})$, for some $\mathfrak{p}$, hence a fortiori $A(\nu, \mathfrak{p}^q) = 0$ for $q > 2c$, and $\sigma_{\mathfrak{p}} = 0$, $\sigma = 0$. Consequently, for the completion of the proof of the Theorem, it is sufficient to demonstrate the following

LEMMA 3. *If* $m > (2^{r-1} + n)nr$, *then* $A_0(\nu, \mathfrak{p}^{2c+1}) > 0$ *for all* ν *in* $J_r(\mathfrak{p})$.

Proof. Put $N(\mathfrak{p}) = p^g$, p being a rational prime number, and let $\mathfrak{p}^l$ be the highest power of $\mathfrak{p}$ dividing p; then $gl \leqq n$ and $l \mid c = fl$, where p^f denotes the highest power of p dividing r.

The numbers of the ring J_r form modulo $\mathfrak{p}^{2c+1}$ an additive Abelian group; let s be its order, then $s \mid N(\mathfrak{p}^{2c+1}) = p^{g(2c+1)} \leq p^{n(2f+1)}$. Since J_r is generated by the r-th powers of all integers, there exist integers $\eta_1, \cdots, \eta_d$ in K and rational integers $q_k > 1$ $(k = 1, \cdots, d)$, with $q_1 \cdots q_d = s$, such that the linear form $x_1\eta_1{}^r + \cdots + x_d\eta_d{}^r$ $(x_k = 0, 1, \cdots, q_k - 1;\ k = 1, \cdots, d)$ uniquely represents all numbers of J_r modulo $\mathfrak{p}^{2c+1}$.

Let m_p denote the smallest number such that every rational integer is congruent to a sum $y_1{}^r + \cdots + y_{m_p}{}^r$ modulo p^q $(q = 1, 2, \cdots)$, where $y_1, \cdots, y_{m_p}$ are rational integers; define

$$\sum_{k=1}^{d} \operatorname{Min}(q_k - 1, m_p) = j.$$

The congruence

$$\lambda_1{}^r + \cdots + \lambda_j{}^r \equiv \nu \pmod{\mathfrak{p}^{2c+1}}$$

has an integral solution $\lambda_1, \cdots, \lambda_j$ in K, whenever ν belongs to $J_r(\mathfrak{p})$. If $(\nu, \mathfrak{p}) = 1$, then the solution is certainly primitive modulo $\mathfrak{p}$; if $\mathfrak{p} | \nu$, then $(\nu - 1, \mathfrak{p}) = 1$; consequently, in both cases, $A_0(\nu, \mathfrak{p}^{2c+1}) > 0$ provided that $m \geq j + 1$. Therefore it is sufficient to prove the inequality

$$(41) \qquad j < (2^{r-1} + 1) nr.$$

Since q_k is a power of p and $q_1 \cdots q_d \leq p^{n(2f+1)}$, we infer that $d \leq n(2f+1)$. On the other hand, it is known that $m_p \leq 4r$ for $r > 3$, $m_p = 4$ for $r = 2, 3$. Moreover, $f = 0$ in case $(p, r) = 1$ and $2f + 1 \leq 3(\log r / \log p)$ in case $p | r$; hence

$$(42) \qquad \frac{j}{nr} \leq \frac{m_p d}{nr} \leq \begin{cases} 12 \dfrac{\log r}{\log p} < 2^{r-1} & (p | r > 4), \\ 4 \leq 2^{r-1} & (r > 2,\ (p, r) = 1 \text{ or } p = r = 3), \\ 2 = 2^{r-1} & (p > r = 2). \end{cases}$$

In the two remaining cases $p = 2$, $r = 2^f$, $f = 1$ or $f = 2$, we set $q_k = 2^{a_k}$ $(k = 1, \cdots, d)$ and assume that the values $a_k = u$ $(u = 1, 2, \cdots, 2f)$ and $a_k > 2f$ occur exactly h_u and h_{2f+1} times. In both cases, $m_2 = 2^{2f} = r^2$, and therefore

$$2^{2f} h_{2f+1} + \sum_{u=1}^{2f} (2^u - 1) h_u = j, \qquad \sum_{u=1}^{2f+1} u h_u \leq n(2f+1),$$

whence

$$(43) \qquad j/nr \leq (r^2 - 1)/r\,(1 + 1/2f) < \tfrac{3}{2} r \leq 2^{r-1} + 1 \qquad (p | r = 2, 4).$$

The assertion (41) follows from (42) and (43); and the proof of the Theorem is now accomplished.

As an immediate consequence of the Theorem, there exists a positive rational integer w depending only upon K and m such that the equation

$$(44) \qquad (\xi_1/w)^r + \cdots + (\xi_m/w)^r = \nu$$

has a solution in totally positive integers $\xi_1, \cdots, \xi_m$ in K, for *all* totally positive integers ν in K, if $m > (2^{r-1} + n) nr$. This particular result can also be found in the following simpler way:

According to (5), we may assume $\nu^{(l)} < C \nu^{(k)}$ $(k, l = 1, \cdots, n)$, where the constant C depends only upon K and r. Since the numbers of K lie everywhere dense in R, we may construct n totally positive numbers $\vartheta_1, \cdots, \vartheta_n$ in

K such that the matrix $(\eta_l^{(k)})$, with $\eta_l = \vartheta_l^r$, lies in any given neighborhood of the unit matrix (e_{kl}); hence we may assume $|\gamma_l^{(k)} - e_{kl}| < 1/Cn$, where $(\gamma_l^{(k)}) = (\eta_k^{(l)})^{-1}$. Then $\nu = a_1\vartheta_1^r + \cdots + a_n\vartheta_n^r$, with

$$a_k = S(\gamma_k\nu) = (1 - 1/Cn)\nu^{(k)} - \sum_{l \neq k} (1/Cn)\nu^{(l)}$$
$$> (1 - 1/Cn - (n-1)/n)\nu^{(k)} > 0 \qquad (k = 1, \cdots, n).$$

Choose a positive rational integer v such that the numbers $v\vartheta_k$ and $v^r\gamma_k$ $(k = 1, \cdots, n)$ are all integral; then $v^r a_k$ is a positive rational integer. Assume now that the Waring-Hilbert Theorem holds for the exponent $m = m_0$, in the field of rational numbers; then $v^r a_k = \sum_{l=1}^{m_0} x_{kl}^r$ with rational integral $x_{kl} \geq 0$ $(k = 1, \cdots, n;\ l = 1, \cdots, m_0)$, and even $x_{kl} > 0$, if v is chosen sufficiently large. It follows that (44) has a solution, if $w = v^2$ and $m \geq m_0 n$. Using the Theorem for $n = 1$, we infer that $m \geq ((2^{r-1} + 1)r + 1)n$ is a sufficient condition for the existence of a solution of (44). This condition is weaker than (2), in case $n > 1$, and it might be suggested that the Theorem remains true, if this condition is substituted for (2). The demonstration of the suggestion can be performed by using sharper estimates in some places of our proof.

In the case $r = 2$, it is known that the Theorem holds even under the condition $m > 4$, independent of n, instead of (2). The question arises whether the lower bound $(2^{r-1} + n)nr + 1$ for m could be replaced by a function of r alone; however, the solution of this new problem seems rather difficult.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

AN UNSOLVED CASE OF THE WARING PROBLEM.*

By IVAN NIVEN.

The Dickson-Pillai-Vinogradow solution [1] of Waring's problem leaves untreated the case in which

$$r = 2^n - q - 2, \tag{1}$$

where

$$3^n = 2^n q + r, \qquad 0 < r < 2^n. \tag{2}$$

The Waring problem is the determination of the value of $g(n)$ such that every positive integer is expressible as a sum of $g(n)$ positive or zero n-th powers, whereas at least one positive integer is not a sum of $g(n) - 1$ n-th powers. The value of $g(n)$ has been determined for $n > 6$, unless r has the value (1). We prove here that in case (1) holds, $g(n)$ has the ideal value I, that is [2]

$$g(n) = I = 2^n + q - 2. \tag{3}$$

By the remark immediately following Theorem 4 of (D) we consider $n > 180$. We shall make use of Lemma 10 of (D), altered slightly to suit our purposes:

*If $n > 180$, $L \leqq 6^n$, and all integers in the interval $(L, L + 2^n)$ are sums of m n-*th *powers, then every integer $\geqq L$ is a sum of $m + q + s - 2$ n-*th *powers.*

The integer s is defined by

$$s = f + 2g, \qquad f = [(4/3)^n], \qquad g = [(5/4)^n], \tag{4}$$

where $[x]$ denotes the greatest integer $\leqq x$. Lemma 10 of (D) has $n \geqq 35$

* Received October 21, 1942.

[1] L. E. Dickson, "Proof of the ideal Waring theorem for exponents 7-180" and "Solution of Waring's problem," *American Journal of Mathematics*, vol. 58 (1936), pp. 521-535. These papers are written with a continuity in the numbering of formulas, sections etc., and so we refer to them jointly as (D).

[2] Thus the values of $g(n)$ for $n > 6$ are complete, as follows (using f as defined in (4)): if $r < 2^n - q$, $g(n) = I$; if $r \geqq 2^n - q$, $g(n) = I + f$ or $I + f - 1$ according as $2^n =$ or $< fq + f + q$.

and the inferred hypothesis that $L \leqq 4^n$. The change in the inequality satisfied by L corresponds to replacing 3 by 6 in the inequality following equation (15) of (D); the resulting inequality is true for $n \geqq 8$.

We write, as in (D),

$$(5) \qquad 4^n = 3^n f + 2^n h + j, \qquad 0 \leqq 2^n h + j < 3^n, \qquad 0 \leqq j < 2^n.$$

Using (1) and (2) we have

$$(6) \qquad 4^n = 2^n(qf + f + h) + j - qf - 2f,$$

so that

$$j \equiv qf + 2f \pmod{2^n}.$$

But also $qf = [(3/2)^n] \cdot [(4/3)^n] < 2^n$ and $2f < 2^n$ so that we have

$$(7) \qquad j = qf + 2f \quad \text{with} \quad h = 2^n - qf - f,$$

or

$$(8) \qquad j = qf + 2f - 2^n \quad \text{with} \quad h = 2^n - qf - f + 1,$$

whichever value of j satisfies the last inequality in (5), the corresponding value of h arising from (6).

We now find an interval $(L, L + 2^n)$, every integer of which is a sum of $2^n - s$ n-th powers; this will enable us to apply the lemma from (D). We use different values of L in the two cases, (7) and (8).

If (7) holds we take $L = 4^n f$. All integers in the interval $(4^n f, 4^n f + 2^n - s - f)$ are clearly sums of $2^n - s$ powers. We rewrite the next integer in the form

$$(9) \quad (f^2 + t)3^n + (fh - tq - t + f + 1)2^n + fj + tq + 2t - 2^n f - s - f + 1,$$

by means of (5), (1) and (2), and the arbitrary integer t is chosen to satisfy

$$(10) \qquad t = [2^n f/(q+1)] - f^2.$$

Note first that t is not negative. For by (7) $2^n \geqq qf + f$ so that $2^n f \geqq f^2(q+1)$. We shall also need the inequalities

$$(11) \qquad t > 2^n f/(q+1) - f^2 - 1,$$

and

$$(12) \qquad t \leqq 2^n f/(q+1) - f^2 = f(2^n - qf - f)/(q+1) < f$$

the last step being a consequence of

$$2^n - qf - f < q + 1 \quad \text{or} \quad 2^n < (q+1)(f+1).$$

Now the integer (9) is clearly a sum of $f(f + h + j - 2^n) + 2t - s + 2$ n-th powers, and this number, by (7) and (12), is less than $2f^2 + 2f - s + 2$. Hence all integers from (9) to $4^n f + 2^n$ are sums of $2f^2 + 3f + 1$ n-th powers. For $n > 180$ this is less than $2^n - s$, since $f^2 < (16/9)^n$ and $s < 2f$.

To complete this argument we must show that the coefficients of 3^n, 2^n and 1 in (9) are not negative. The coefficient of 3^n is positive since t is not negative. The coefficient of 2^n exceeds $fh - t(q+1)$, which is not negative since the first inequality in (12) may be written $t < fh/(q+1)$. Finally we have

$$\begin{aligned} &fj + tq + 2t - 2^n f - s - f + 1 \\ &> f^2 q + 2f^2 + 2^n f - f^2 q - f^2 - q - 1 - 2^n f - s - f + 1 \\ &= f^2 - q - s - f, \end{aligned}$$

by applying (7) and (11) to j and t respectively. An easy computation shows this to be positive for $n > 180$.

If (8) holds we take $L = 4^n u$, where u is an integer to be specified. As before we take the interval $(4^n u, 4^n u + 2^n - s - u)$ for granted, and begin with $N = 4^n u + 2^n - s - u + 1$. We have, by (5),

$$N = 3^n(uf) + 2^n(uh + 1) + uj - s - u + 1. \tag{13}$$

First we suppose that $j > f/2$. Taking $u = 4$ we see that N in (13) is a sum of $8f - s + 2$ n-th powers, by (8). Hence all integers in the interval $(N, N + s + 3)$ are sums of $8f + 5$ powers, which is less than $2^n - s$ for $n > 180$. Again we must demonstrate that the coefficients of 3^n, 2^n and 1 in (13) are not negative. Our hypothesis on j enables us to write the only inequality needed,

$$uj - s - u + 1 = 4j - s - 3 > 2f - s - 3 > 0.$$

On the other hand suppose that $j \leqq f/2$. Then choose u to satisfy

$$u = [q/h] + 1$$

so that u is positive, and we have

$$uh > q, \qquad uh \leqq q + h. \tag{14}$$

Since $j + h = f + 1$, our hypothesis on j implies $h > f/2$ so that the second inequality in (14) implies

$$u < 2q/f + 1 < f. \tag{15}$$

We can write (13) in the form

$$N = 3^n(uf + 1) + 2^n(uh - q) + uj - s - u + q + 3,$$

so that N is seen to be a sum of $u(f + h + j - 1) - s + 4$ n-th powers. By (8) this equals $u(2f) - s + 4$, which is less than $2f^2 - s + 4$, by (15). Hence any integer in the interval $(N, N + u + s - 1)$ is a sum of $2f^2 + u + 3$ n-th powers, and (15) implies that this does not exceed $2f^2 + f + 3$, which in turn is less than $2^n - s$. The coefficient of 2^n in N is positive by the first inequality in (14), and the coefficient of 1 is

$$uj - s - u + q + 3 > -s - u + q > -s - f + q > 0,$$

by (15) and the definitions of q, s and f.

Thus we have exhibited an interval $(L, L + 2^n)$, every integer of which is a sum of $2^n - s$ n-th powers. In case of (7) we had $L = 4^nf$, in case (8) $L = 4^nu$ with $u = 4$ and $u < f$ in the two parts of the proof. The lemma quoted from (D) is applicable since $4^nf < (16/3)^n < 6^n$. To complete our proof of (3) we have simply to show that every integer $N < 4^nf$ is a sum of $I = 2^n + q - 2$ n-th powers. This we proceed to do.

We separate the work into cases, since no unified treatment seems available. The integers $< 3^n$ are easily handled, so we take N between 3^n and 4^nf. All integers are given by

$$N = 4^nw + 3^nx + 2^ny + z \tag{16}$$
$$(0 \leqq w \leqq f - 1,\ 0 \leqq x \leqq f,\ 0 \leqq y \leqq q,\ 0 \leqq z \leqq 2^n - 1).$$

Case 1. $3^n \leqq N < 4^nf$, $z \leqq 2^n - 2f - 1$. Then N is a sum of $x + y + z + w$ n-th powers, and this is at most

$$f + q + 2^n - 2f - 1 + f - 1 = I.$$

Case 2. $3^n \leqq N < 4^n$, $z \geqq 2^n - 2f$. The first hypothesis implies $w = 0$, and we can write

$$N = (x - t)3^n + (y + qt + t)2^n + z - qt - 2t,$$

with the integer t to be specified. We need non-negative coefficients here, so we must have $t \leqq x$ and $t \leqq z/(q + 2)$. These are satisfied if we choose

$$t = \min\{x, [z/(q + 2)]\}.$$

Now N is a sum of $x+y+z-2t$ n-th powers. If $t=x$ we have

$$x+y+z-2t \leqq y+z-1 \leqq I,$$

since $x>0$. If $t=[z/(q+2)]$ we have

$$x+y+z-2t<f+q+2^n-1-2z/(q+2)+2 \leqq I$$

since

$$2z \geqq 2^n+2^n-4f>qf+2^n-4f>(q+2)(f+3).$$

Case 3. $4^n \leqq N<4^n f$, $z \geqq 2^n-2f$, $w \leqq x-3$. Equations (1) and (2) enable us to write

$$N=w4^n+3^n+2^n\{y+(x-1)(q+1)\}+z-(x-1)(q+2).$$

This is a sum of $w+y+z-x+2$ n-th powers, and our hypothesis on w implies that this does not exceed I. The coefficient of 1 in N is positive since

$$\begin{aligned} z-(x-1)(q+2) &\geqq 2^n-2f-(f-1)(q+2) \\ &=(2^n-qf)+(q-4f)+2>0. \end{aligned}$$

Case 4. $4^n \leqq N<4^n f$, (7), $z \geqq 2^n-2f$, $w \geqq x-2$, $w \geqq 3$. We can write

$$\begin{aligned} N=3^n(x+wf+t)+2^n(y+wh-tq-t+w+1) \\ +z+wj+tq+2t-2^n(w+1) \end{aligned}$$

and we define t by the equation

$$t=[(y+wh)/q]$$

so that

(17) $$tq+q>y+wh \geqq tq.$$

The second part of (7) implies that $h \leqq q$ whence we have

(18) $$t \leqq [(q+wq)/q]=w+1.$$

We again use (7) to conclude that N is a sum of

$$x+y+z+w+2wf+2t+1-2^n$$

n-th powers, and the inequalities among the hypotheses of the case and (18) show that this does not exceed I. The coefficient of 2^n is not negative because

of (17) and (18). Finally we have

$$z + wj + tq + 2t - 2^n(w + 1) \geqq 2^n - 2f + w(j - 2^n) + tq - 2^n$$
$$> -2f + w(j - 2^n) + y + wh - q = y + wf - q - 2f.$$

Thus we see that our method is not adequate in case $y + wf < q + 2f$ but in this case we have

$$\begin{aligned} x + y + z + w &< x + z + w + q + 2f - wf \\ &\leqq w + 2 + 2^n - 1 + w + q + 2f - wf \\ &= I + 2w + 2f - wf + 3 < I, \end{aligned}$$

where the last inequality follows from $w \geqq 3$.

Case 5. $4^n \leqq N < 4^n f$, (7), $z \geqq 2^n - 2f$, $w \geqq x - 2$, $w = 1$ or 2. The last two hypotheses imply that $x \leqq 4$. If $z \leqq 2^n - 8$ we have

$$x + y + z + w \leqq 4 + q + 2^n - 8 + 2 = I.$$

Consequently we can take $z > 2^n - 8$ for the remainder of this case.

First we assume that $y + h < q$. By (7) it is seen that $h = 2^n - j + f$ whence $h > f$ so that $y < q - f$. Hence we have

$$x + y + z + w \leqq 4 + q - f + 2^n - 1 + 2 < I.$$

If on the other hand $y + h \geqq q$, we write

$$\begin{aligned} N = 4^n(w - 1) &+ 3^n(x + f + 1) \\ &+ 2^n(y + h - q + 1) + z + j - 2^n + q + 2 - 2^n \end{aligned}$$

which is easily shown to be a sum of I n-th powers. The coefficient of 2^n is clearly positive, and we also have

$$\begin{aligned} &z + j - 2^n + q + 2 - 2^n \\ &\quad \geqq 2^n - 7 + qf + 2f - 2^n + q + 2 - 2^n \\ &\quad = (qf + f + q + 1 - 2^n) + (f - 6) > 0. \end{aligned}$$

Case 6. $4^n \leqq N < 4^n f$, (8), $z \geqq 2^n - 2f$, $w \geqq x - 2$. We divide this case into three parts.

If $y + wh \geqq q$ we can write

$$N = 3^n(x + wf + 1) + 2^n(y + wh - q) + z + wj - 2^n + q + 2.$$

If $z + wj \geqq 2^n$ we can write

$$N = 3^n(x + wf) + 2^n(y + wh + 1) + z + wj - 2^n.$$

The necessary inequalities are obtained as before.

If $y + wh \leqq q - 1$ and $z + wj \leqq 2^n - 1$, these inequalities add to give $y + z + w(f + 1) \leqq I$, and we have

$$x + y + z + w \leqq w + 2 + y + z + w < y + z + w(f + 1) \leqq I \quad \text{since} \quad w > 0.$$

Thus our six cases are completely treated, and the various hypotheses cover all integers in (16).

PURDUE UNIVERSITY.

THE FAN INTEGRALS INTERPRETED AS MEASURES IN A PRODUCT-SPACE.*

By A. J. Ward.

In a recent paper [1] S. C. Fan has defined four related integrals of a function $f(x)$, in general non-measurable, on a set E. If the function and set concerned are measurable, these all reduce to the Lebesgue integral, or rather to the analogue of the Lebesgue integral for a general measure-function. Now it is well known that the Lebesgue integral of a non-negative function is the measure (in a space of one higher dimension) of the ordinate-set of the function.[2] In this paper we prove an analogous result for the Fan integrals, showing that they may be regarded as upper or lower measures of the ordinate-set of $f(x)$, and examine some of the theorems of *SF* in the light of this conception. We then consider more especially the case when the basic measure-function is regular,[3] showing that in this case the Fan integrals may be expressed as Lebesgue integrals of certain measurable functions associated with $f(x)$.

1. As in *SF*, we consider an upper-measure function $\bar{m}(E)$, defined, finite, and non-negative for all subsets of a given fixed set E_0, and subject to the following conditions: [4]

(a) If $E_1 \subset E_2$, then $\bar{m}(E_1) \leq \bar{m}(E_2)$.

---

* Received May 20, 1942.

[1] S. C. Fan, "Integration with respect to an upper-measure function," *American Journal of Mathematics*, vol. 63 (1941), pp. 319-337. This paper will be referred to as SF. Theorem 1 SF denotes Theorem 1 of Fan's paper, and so on.

[2] By the ordinate-set of $f(x)$ on E we mean the set of points (x, y) such that $x \in E$, $0 \leq y \leq f(x)$.

[3] An upper measure $\bar{m}$ is regular if to each set E (of finite upper measure) there corresponds a set H, measurable $(\bar{m})$ and including E, such that $\bar{m}H = \bar{m}E$, and therefore also $\bar{m}(XH) = \bar{m}(XE)$ for every set X measurable $(\bar{m})$ (such a set will be called an equimeasurable cover of E). The most important property of regular upper measures is the following. If (E_n) is a sequence of sets such that $E_n \subset E_{n+1}$ for each n, then $\bar{m}(\sum_{n=1}^{\infty} E_n) = \lim_{n\to\infty} \bar{m}E_n$. See C. Carathéodory, *Vorlesungen ueber reelle Funktionen* (2nd edition, Leipzig 1927), pp. 258 ff., especially Satz 15, 270.

[4] The set E_0, and its subsets, may be composed of elements of any nature; a typical element of E_0 will always be denoted by x. As we do not consider any questions of topology in E_0, we do not require Carathéodory's fourth axiom (*loc. cit.* 239).

(b) For any two sets E, E',

$$\bar{m}(E+E')+\bar{m}(EE')\leq \bar{m}E+\bar{m}E'.$$

(c) For any sequence of sets (E_n),

$$\bar{m}\left(\sum_{n=1}^{\infty}E_n\right)\leqq\sum_{n=1}^{\infty}\bar{m}E_n.$$

We assume also that for the empty set O, $\bar{m}(O)=0$.

Conditions (a) and (b) suffice to allow us to define a corresponding lower measure $\underline{m}(E)$, as $\bar{m}(E_0)-\bar{m}(E_0-E)$, with the usual properties. If $\underline{m}(E)=\bar{m}(E)$, E is called measurable $(\bar{m})$. Measurable sets have the usual properties, and (c) ensures that the measure-function is completely additive over measurable sets. Again, given any subset E_1 of E_0, we may define (for subsets of E_1) *lower measure relative to* E_1, as $\bar{m}(E_1)-\bar{m}(E_1-E)$, and speak of measurability relative to E_1.

For simplicity we consider only bounded functions $f(x)$. By the addition of a constant we may then suppose that $0\leq f(x)<M$, where M is some constant. In this case the most convenient definitions of the Fan integrals are [5]

$$\int_E f\,d\bar{\mu}^*=\int_0^M\bar{m}[E(f>y)]dy,$$

and

$$\int_E f\,d\bar{\mu}=M\cdot\bar{m}(E)-\int_0^M\bar{m}[E(f<y)]dy,$$

$\int_E f\,d\underline{\mu}^*$ and $\int_E f\,d\underline{\mu}$ being defined similarly in terms of the lower measure $\underline{m}$. We remark that if $S\subset E$ and $\bar{m}S=\bar{m}E$, then

$$\int_S f\,d\bar{\mu}^*\leq\int_E f\,d\bar{\mu}^*\quad\text{and}\quad\int_S f\,d\bar{\mu}\geq\int_E f\,d\bar{\mu}.$$

We may express all these integrals in terms of $\bar{\mu}^*$ integrals. Let us write $f_1(x)=f(x)$ on E and $f_1(x)=0$ on E_0-E, $f_2(x)=f(x)$ on E and $f_2(x)=M$ on E_0-E, $g(x)=M-f(x)$, and $g_1(x)=M-f_1(x)$. Then [6]

$$\int_0^M\bar{m}[E(f<y)]dy=\int_0^M\bar{m}[E(g>M-y)]dy=\int_0^M\bar{m}[E(g>y)]dy$$

(changing y to $M-y$), so that

$$\int_E f\,d\bar{\mu}=M\cdot\bar{m}(E)-\int_E g\,d\bar{\mu}^*. \tag{1}$$

---

[5] Cf. equations (4) (321) and (16) (328), SF. We remark that on the right hand side we have ordinary Riemann integrals, the integrand being in each case a monotone function of y.

[6] Cf. Theorem 7 SF.

Similarly, since

$$\underline{m}[E(f > y)] = \underline{m}[E_0(f_1 > y)] = \bar{m}E_0 - \bar{m}[E_0(g_1 \geq M - y)]$$
$$= \bar{m}E_0 - \bar{m}[E_0(g_1 > M - y)]$$

for almost all positive y,[7] we deduce that

$$\int_E f\, d\mu^* = M \cdot \bar{m}(E_0) - \int_{E_0} g_1 d\bar{\mu}^*. \tag{2}$$

Finally,

$$\underline{m}[E(f < y)] = \underline{m}[E_0(f_2 < y)] \ \ (\text{if } y \leq M) = \bar{m}E_0 - \bar{m}[E_0(f_2 \geq y)]$$

so that

$$\int_E f\, d\underline{\mu} = \int_{E_0} f_2\, d\bar{\mu}^* - M[\bar{m}(E_0) - \underline{m}(E)]. \tag{3}$$

The last expression may be simplified if there exists an $\bar{m}$-measurable set $K \subset E$ such that $\bar{m}K = \underline{m}E$.[8] For then (cf. Theorem 2 SF)

$$\int_{E_0} f_2(x)\, d\bar{\mu}^* = \int_K f_2(x)\, d\bar{\mu}^* + \int_{E_0 - K} f_2(x)\, d\bar{\mu}^*$$
$$= \int_K f(x)\, d\bar{\mu}^* + M(\bar{m}E_0 - \underline{m}E)$$

since $\bar{m}[(E_0 - K)(f_2 > y)] \geq \bar{m}(E_0 - E)$ for all $y < M$. Hence in this case

$$\int_E f\, d\mu = \int_K f\, d\bar{\mu}^*. \tag{4}$$

Similarly

$$\int_E f\, d\underline{\mu}^* = \int_K f\, d\bar{\mu}. \tag{5}$$

2. We now define an upper measure, which we shall denote by $\overline{m \times L_1}$, or by $\bar{\boldsymbol{m}}$, in the Cartesian product-space $E_0 \times \langle 0, M\rangle$. Let $\boldsymbol{E}$ be any set in this space, and let it be covered by a sequence of sets $\boldsymbol{E}_n$ each of the form $E_n \times J_n$, where E_n is a subset of E_0 and J_n is a measurable set (in the ordinary Lebesgue sense) in the interval $\langle 0, M\rangle$. Then $\bar{\boldsymbol{m}}\boldsymbol{E}$ is defined as the lower

[7] SF, 321, Remark (3).

[8] Two important particular cases are (I) if the measure is regular; (II) for any measure, if E is measurable ($\bar{m}$).

bound of $\sum_{n=1}^{\infty} (\bar{m}E_n) \cdot | J_n |$ for all such coverings.[9] $\bar{\boldsymbol{m}}\boldsymbol{E}$ is clearly defined, finite, and non-negative for all subsets of $E_0 \times \langle 0, M \rangle$.

THEOREM 1. *$\bar{\boldsymbol{m}}\boldsymbol{E}$ satisfies the conditions* (a), (b) *and* (c) *of* **1**.

(a) and (c) are clearly satisfied; it remains to prove (b). Let $\boldsymbol{E}$ and $\boldsymbol{E}'$ be any two sets of the product-space, covered by sequences $\sum_{n=1}^{\infty} (E_n \times J_n)$ and $\sum_{n=1}^{\infty} (E'_n \times J'_n)$ respectively, such that $\sum_{n=1}^{\infty} (\bar{m}E_n) \cdot | J_n | - \bar{\boldsymbol{m}}\boldsymbol{E}$ and $\sum_{n=1}^{\infty} (\bar{m}E'_n) \cdot | J'_n | - \bar{\boldsymbol{m}}(\boldsymbol{E}')$ are each less than a given positive number ϵ. Take any integer N such that $\sum_{n>N} (\bar{m}E_n) \cdot | J_n | + \sum_{n>N} (\bar{m}E'_n) \cdot | J'_n | < \epsilon$, and consider the 2^{2N} non-overlapping "elementary subsets" obtained by forming the product of any selection from the sets $J_1, J_2, \cdots, J_N, J'_1, \cdots, J'_N$ and the complements of the remaining sets of index $\leq N$. Arrange these elementary subsets[10] in any order as $K_1, K_2, \cdots, K_P$, say, where $P = 2^{2N}$. Any set J_n, where $n \leq N$, is the sum of a certain selection of the sets K_p.

Since the sets K_p are measurable and non-overlapping, we may, for all $n \leq N$, replace $E_n \times J_n$ by $(E_n \times J_nK_1) + (E_n \times J_nK_2) + \cdots + (E_n \times J_nK_P)$ without altering the sum $\Sigma(\bar{m}E_n) \cdot | J_n |$. For any given $p \leq P$, let $r, s, \cdots, t$ be those indices such that $J_r, J_s, \cdots, J_t$ contain K_p. The sets $(E_n \times J_nK_p)$, $n = 1, 2, \cdots, N$, can be replaced by $(E_r + E_s + \cdots + E_t) \times K_p$, since $J_nK_p = K_p$ for $n = r, s, \cdots, t$ and $J_nK_p = 0$ for the remaining values of n; and by (b), **1**, we have not increased the sum $\Sigma(\bar{m}E_n) \cdot | J_n |$, since $\bar{m}(E_r + \cdots + E_t) \leq \bar{m}E_r + \cdots + \bar{m}E_t$. We may work similarly with the covering $\Sigma(E'_n \times J'_n)$. Thus we may replace the original coverings $\Sigma(E_n \times J_n)$ and $\Sigma(E'_n \times J'_n)$ by new coverings

$$(F_1 \times K_1) + (F_2 \times K_2) + \cdots + (F_P \times K_P) + \sum_{n>N} (E_n \times J_n)$$

and

$$(F'_1 \times K_1) + (F'_2 \times K_2) + \cdots + (F'_P \times K_P) + \sum_{n>N} (E'_n \times J'_n),$$

say, such that

$$\sum_{p=1}^{P} (\bar{m}F_p) \cdot | K_p | \leq \sum_{n=1}^{N} (\bar{m}E_n) \cdot | J_n |$$

---

[9] $| J |$ denotes the upper Lebesgue measure of any linear set J. We use the notation $\overline{m \times L_1}$ for our upper measure when we are comparing it with some other measure in the product-space: otherwise we use $\bar{\boldsymbol{m}}$ for brevity.

[10] Some of the subsets may of course be empty, but this does not affect the argument.

and

$$\sum_{p=1}^{P} (\bar{m}F'_p) \cdot |K_p| \leq \sum_{n=1}^{N} (\bar{m}E'_n) \cdot |J'_n|.$$

It is clear that $\boldsymbol{E} + \boldsymbol{E}'$ is covered by

$$\sum_{p=1}^{P} [(F_p + F'_p) \times K_p] + \sum_{n>N} (E_n \times J_n) + \sum_{n>N} (E'_n \times J'_n),$$

and (since $K_pK_q = 0$ for $p \neq q$) $\boldsymbol{EE}'$ is covered by

$$\sum_{p=1}^{P} (F_pF'_p \times K_p) + \sum_{n>N} (E_n \times J_n) + \sum_{n>N} (E'_n \times J'_n).$$

Hence

$$\begin{aligned} \bar{\boldsymbol{m}}(\boldsymbol{E} + \boldsymbol{E}') + \bar{\boldsymbol{m}}(\boldsymbol{EE}') &\leq \sum_{p=1}^{P} [\bar{m}(F_p + F'_p) + \bar{m}(F_pF'_p)] \cdot |K_p| + 2\epsilon \\ &\leq \sum_{p=1}^{P} [\bar{m}(F_p) + \bar{m}(F'_p)] \cdot |K_p| + 2\epsilon \\ &\leq \sum_{n=1}^{N} (\bar{m}E_n) \cdot |J_n| + \sum_{n=1}^{N} (\bar{m}E'_n) \cdot |J'_n| + 2\epsilon \\ &\leq \bar{\boldsymbol{m}}(\boldsymbol{E}) + \bar{\boldsymbol{m}}(\boldsymbol{E}') + 4\epsilon, \end{aligned}$$

from which the required result follows at once. We may now define $\underline{m \times L_1}(\boldsymbol{E})$, or $\underline{\boldsymbol{m}}(\boldsymbol{E})$, as

$$\bar{\boldsymbol{m}}[E_0 \times \langle 0, M\rangle] - \bar{\boldsymbol{m}}[(E_0 \times \langle 0, M\rangle) - \boldsymbol{E}].$$

In future we write J_0 for the interval $\langle 0, M\rangle$.

THEOREM 2. *Let* $\boldsymbol{E}$ *be the ordinate-set of* $f(x)$ *on* E. *Then*

(i) $\int_E f(x)\, d\bar{\mu}^* = \overline{m \times L_1}(\boldsymbol{E})$;

(ii) $\int_E f(x)\, d\underline{\mu}^* = \underline{m \times L_1}(\boldsymbol{E})$;

(iii) $\int_E f(x)\, d\bar{\mu}$ *is the lower measure of* $\boldsymbol{E}$ *relative to* $E \times J_0$;

(iv) $\int_E f(x)\, d\underline{\mu}$ *is the lower measure of* $\boldsymbol{E}$ *relative to* $\boldsymbol{E} + (E_0 - E) \times J_0$.

Let $\Sigma(E_n \times J_n)$ be any covering of $\boldsymbol{E}$. Write $\mu_n(y) = \bar{m}(E_n)$ if y is in J_n, and $\mu_n(y) = 0$ otherwise. For any y_0, those sets E_n for which $y_0 \in J_n$ must cover the section of $\boldsymbol{E}$ by the line $y = y_0$, that is, the set $E(f \geq y_0)$. It follows, since $\bar{m}$ satisfies the condition (c), that

$$\sum_n \mu_n(y_0) \geq \bar{m}[E(f \geq y_0)] \geq \bar{m}[E(f > y_0)].$$

Now, for each n, $\int_0^M \mu_n(y)\,dy = (\bar{m}E_n) \cdot |J_n|$. Hence, if $\sum_n (\bar{m}E_n) \cdot |J_n|$ is finite, $\sum_n \mu_n(y)$ must be Lebesgue summable [11] in J_0 and we have

$$\sum (\bar{m}E_n) \cdot |J_n| = \int_0^M \sum_n \mu_n(y) \cdot dy \geq \int_0^M \bar{m}[E(f > y)]dy.$$

It follows that $\int_E f\, d\bar{\mu}^* \leq \boldsymbol{mE}$.

On the other hand, given $\epsilon > 0$, we can form a division of J_0 by points $0 = y_0 < y_1 < y_2 < \cdots < y_N = M$ such that

$$\sum_{n=0}^{N-1} \bar{m}[E(f > y_n)] \cdot (y_{n+1} - y_n) < \int_E f\, d\bar{\mu}^* + \epsilon.$$

$\boldsymbol{E}$ is clearly covered by the sets $E(f > y_n) \times \langle y_n \cdot y_{n+1} \rangle$, $n = 0, 1, \cdots, N-1$, together with $E \times (y = 0)$, and so

$$\bar{\boldsymbol{m}}\boldsymbol{E} < \int_E f\, d\bar{\mu}^* + \epsilon.$$

Since ϵ is arbitrary, we have proved part (i) of the theorem.

We remark that it follows, in particular, that $\bar{\boldsymbol{m}}(E \times J_0) = M.\bar{m}E$. Hence, if E is measurable $\bar{m}$ relative to E_1, then $E \times J_0$ is measurable $\bar{\boldsymbol{m}}$ relative to $E_1 \times J_0$.

We now turn to part (ii); it is required to prove that

$$\bar{\boldsymbol{m}}(E_0 \times J_0 - \boldsymbol{E}) = M \cdot \bar{m}E_0 - \int_E f\, d\underline{\mu}^* = \int_{E_0} g_1\, d\bar{\mu}^*,$$

by (2) 1.

Now $E_0 \times J_0 - \boldsymbol{E}$ is the set of all points (x, y) such that

$$0 \leq y \leq M \text{ if } x \text{ is in } E_0 - E,$$
$$f(x) < y \leq M \text{ if } x \text{ is in } E.$$

It is clear that we may add the points $[x, f(x)]$, for x in E (thus changing the last inequality to $f(x) \leqq y \leqq M$), without altering the $\bar{\boldsymbol{m}}$ upper measure. We then obtain a set which is congruent with the ordinate-set of g_1 on E_0, being in fact obtained by a reflection of this set in the line $y = \frac{1}{2}M$, and which is easily seen to have the same upper measure. Hence we obtain the required equation

$$\bar{\boldsymbol{m}}(E_0 \times J_0 - \boldsymbol{E}) = \int_{E_0} g_1\, d\bar{\mu}^*$$

by part (i).

---

[11] In particular, $\sum_n \mu_n(y)$ must converge for almost all y.

Parts (iii) and (iv) of the theorem follow similarly from equations (1) and (3) of **1**.

3. Theorem 2, part (i), can be viewed in an interesting way as a relation between two upper measures. It is natural to define, in the (x, y) space, $\overline{m \times J_1}(\boldsymbol{E})$, the product of $\bar{m}$ and Jordan measure, as the lower bound of $\sum_{n=1}^{N} \bar{m}(E_n) \cdot | J_n |$ for all finite coverings of $\boldsymbol{E}$ by sets $E_n \times J_n$, where J_n is Jordan measurable (in particular J_n may be taken as an interval). A proof similar to that of Theorem 1 shows that $\overline{m \times J_1}$ upper measure satisfies conditions (a) and (b), though not (c); so that we may speak of lower measure $\underline{m \times J_1}$. It is clear that

$$\underline{m \times J_1}(\boldsymbol{E}) \leq \underline{m \times L_1}(\boldsymbol{E}) \leq \overline{m \times L_1}(\boldsymbol{E}) \leq \overline{m \times J_1}(\boldsymbol{E})$$

and that the two upper measures are not the same in general. However, the proof of Theorem 2 (i) shows that *the* $\overline{m \times J_1}$ *and* $\overline{m \times L_1}$ *upper measures of an ordinate-set are equal.*

We now consider the relation of our measure to the Ulam-Hahn product measure [12] which we shall denote for the moment by $U\boldsymbol{m}$. Let $\mathfrak{X}$ be the class of sets measurable $\bar{m}$ and $\mathfrak{L}_1$ the class of sets measurable in the ordinary Lebesgue sense in J_0. As remarked above, any set of the form $E \times J_0$, where E is in $\mathfrak{X}$, is measurable $\overline{m \times L_1}$ and $\overline{m \times L_1}(E \times J_0) = \bar{m}E \cdot | J_0 |$. The same is obviously true for any set of the form $E \times J$, where J is an interval. It follows at once that it remains true for sets of the form $E \times J$ where E is in $\mathfrak{X}$ and J is in $\mathfrak{L}_1$. The sets measurable $\overline{m \times L_1}$ form an additive class and the measure $\overline{m \times L}$ is completely additive in that class. Hence any set $\boldsymbol{E}$ measurable $(\mathfrak{X}\mathfrak{L}_1)$ is also measurable $\overline{m \times L_1}$, and $\overline{m \times L_1}(\boldsymbol{E}) = U\boldsymbol{m}(\boldsymbol{E})$. Finally, any subset of a set of zero $U\boldsymbol{m}$-measure is also, by the above argument, of zero $\overline{m \times L_1}$ measure, and so we have further:

Any set $\boldsymbol{E}$ *measurable* $(\mathfrak{X}\mathfrak{L}_1)$ *is also measurable* $\overline{m \times L_1}$ *and* $\overline{m \times L_1}(\boldsymbol{E}) = U\boldsymbol{m}(\boldsymbol{E})$.

The converse is not in general true, as may be seen by the following example.

Let E_0 be the set of real numbers $0 \leq x \leq 1$ and J_0 the set $0 \leq y \leq 1$; write for $E \subset E_0$, $\bar{m}(E) = | E |^{1/2}$. It is easily verified that this upper measure satisfies the conditions (a), (b) and (c), but that the only sets measurable $\bar{m}$

[12] S. Saks, *Theory of the Integral* (Warsaw, 1937), pp. 82-88. We adopt the notation there used.

are, firstly, sets N such that $\bar{m}N = |N| = 0$, and secondly their complements $E_0 - N$. Then all sets in the product-space which are measurable $(\mathcal{X}\mathcal{L}_1)$ are of the form $(E_0 - N) \times J + \boldsymbol{N}$, where $\bar{m}N = 0$, J is measurable $\mathcal{L}_1$, and $\boldsymbol{N}$ is a subset of $N \times J_0$. For the sets of this form constitute an additive class which includes all sets of the form $E \times J$ where E is in $\mathcal{X}$ and J is in $\mathcal{L}_1$. It is also clear that the $U\boldsymbol{m}$-measure of such a set is equal to $|J|$. The sets measurable $(\overline{\mathcal{X}\mathcal{L}_1})$ are obtained by forming the sum of any set measurable $(\mathcal{X}\mathcal{L}_1)$ and any subset of a set measurable $(\mathcal{X}\mathcal{L}_1)$ with zero $U\boldsymbol{m}$-measure. Thus all sets measurable $(\overline{\mathcal{X}\mathcal{L}_1})$ are of the form

$$(E_0 - N) \times J + \boldsymbol{N}_1 + \boldsymbol{N}_2,$$

where N, J are as before, $\boldsymbol{N}_1$ is a subset of $N \times J_0$, and $\boldsymbol{N}_2$ is a subset of $E_0 \times J_2$, say, where $|J_2| = 0$. Now consider the diagonal set $0 \leq x = y \leq 1$. It cannot be expressed in the above form and is therefore not measurable $(\overline{\mathcal{X}\mathcal{L}_1})$. It is however easily verified (covering by the sets $n/k \leqq x, y \leqq (n+1)/k$, $n = 0, 1, \cdots, k-1$) that this set has $\overline{m \times L_1}$ measure zero, and is therefore measurable $\overline{m \times L_1}$.

4. We now return to the Fan integrals. Theorem 2 shows that the integrability $(\bar{\mu})$ of f over E is equivalent to the measurability $(\overline{m \times L_1})$ of the ordinate-set of f on E, relative to $E \times J_0$.[13] (There does not, however, appear to be any such simple interpretation of integrability (μ), if E is not measurable.)

In the light of this remark, the additivity of the integral over relatively measurable subsets of E[14] is seen to correspond to the fact that, if E_n is measurable $\bar{m}$ relative to E, then $E_n \times J_0$ is measurable $\bar{\boldsymbol{m}}$ relative to $E \times J_0$. The ordinate-sets of f on the various sets E_n are 'separated' by being contained in the relatively measurable sets $E_n \times J_0$.

We next consider Theorem 11 SF, which states—in our language—that a necessary and sufficient condition that the ordinate-set of f on E should be measurable $\bar{\boldsymbol{m}}$ relative to $E \times J_0$ is that the function f should be measurable $\bar{m}$ relative to E. The necessary condition is now seen to be a special case of the following analogue of Fubini's theorem.

THEOREM 3. *Let* $\boldsymbol{E}$ *be any set measurable* $\bar{\boldsymbol{m}}$. *For any* y, *let* $E(y)$ *be the set of* x *such that* (x, y) *is in* $\boldsymbol{E}$. *Then* $E(y)$ *is measurable* $\bar{m}$ *for almost all* y, *and*

$$\int_{J_0} \bar{m}E(y) \cdot dy = \bar{\boldsymbol{m}}\boldsymbol{E}.$$

---

[13] In fact, it is equivalent to measurability $\overline{m \times J_1}$, which is stronger.

[14] Theorem 2 SF and the corresponding theorem for μ^* integrals.

The proof is similar to that of Theorem 2. Since $\bar{\boldsymbol{m}}\boldsymbol{E} + \bar{\boldsymbol{m}}(E_0 \times J_0 - \boldsymbol{E}) = M \cdot \bar{m}E_0$, we can, given $\epsilon > 0$, find sequences of sets $\sum_n (E_n \times J_n)$ and $\sum_n (E'_n \times J'_n)$, covering $\boldsymbol{E}$ and $E_0 \times J_0 - \boldsymbol{E}$, respectively, such that

$$\sum_n \bar{m}(E_n) \cdot | J_n | < \bar{\boldsymbol{m}}\boldsymbol{E} + \epsilon \tag{6}$$

and

$$\sum_n \bar{m}(E'_n) \cdot | J'_n | < M \cdot \bar{m}E_0 - \bar{\boldsymbol{m}}\boldsymbol{E} + \epsilon. \tag{7}$$

Define $\mu_n(y)$ as in Theorem 2, and similarly $\mu'_n(y)$ for the set $E'_n \times J'_n$. As in Theorem 2, we have, for any y,

$$\Sigma\mu_n(y) \geq \bar{m}E(y) \tag{8}$$

and

$$\Sigma\mu_n'(y) \geq \bar{m}[E_0 - E(y)] = \bar{m}E_0 - \underline{m}E(y). \tag{9}$$

Now $\Sigma\mu_n(y)$ and $\Sigma\mu'_n(y)$ are, as before, finite almost everywhere in J_0 and Lebesgue summable. Denoting by $\int d\bar{\lambda}^*$ the Fan integral with respect to Lebesgue measure, we now have, from (8) and (9),

$$\Sigma\bar{m}(E_n) \cdot | J_n | = \int_{J_0} \Sigma\mu_n(y)\,dy = \int_{J_0} \Sigma\mu_n(y)\,d\bar{\lambda}^* \geq \int_{J_0} \bar{m}E(y)\,d\bar{\lambda}^*$$

and

$$\int_{J_0} \underline{m}E(y)\,d\lambda \geq \int_{J_0} [\bar{m}E_0 - \Sigma\mu'_n(y)]\,d\bar{\lambda} = M \cdot \bar{m}E_0 - \int_{J_0} \Sigma\mu_n'(y)\,dy$$
$$= M \cdot \bar{m}E_0 - \Sigma\bar{m}(E'_n) \cdot | J'_n |.$$

From (6) and (7) we now obtain

$$\bar{\boldsymbol{m}}(\boldsymbol{E}) - \epsilon < \int_{J_0} \underline{m}E(y)\,d\lambda \leq \int_{J_0} \bar{m}E(y)\,d\bar{\lambda} \leq \int_{J_0} \bar{m}E(y)\,d\bar{\lambda}^* < \bar{\boldsymbol{m}}(\boldsymbol{E}) + \epsilon.$$

Since ϵ is arbitrarily small, $\bar{m}E(y)$ must be integrable $(\bar{\lambda})$. It is therefore measurable (L_1) as a function of y,[15] and the Fan integrals reduce to ordinary Lebesgue integrals. Similarly $\underline{m}E(y)$ is measurable (L_1). We therefore have

$$\int_{J_0} \underline{m}E(y)\,dy = \int_{J_0} \bar{m}E(y)\,dy = \bar{\boldsymbol{m}}(\boldsymbol{E})$$

from which we see that $\bar{m}E(y) = \underline{m}E(y)$ for almost all y.[16]

5. The conditions (b) and (c), satisfied by $\bar{\boldsymbol{m}}$ upper measure, show at

[15] Theorem 11 SF.

[16] The above proof is essentially the same as a standard proof of the ordinary Fubini theorem (C. Carathéodory, *loc. cit.*, 621 ff. We have, however, given the proof in full as it affords an interesting application of the Fan integrals.

once that if $\Sigma E_n = E$, and $f(x) \geq 0$ for all x, then, whether the family of sets (E_n) is finite or enumerable,

$$\Sigma \int_{E_n} f \, d\bar{\mu}^* \geq \int_E f \, d\bar{\mu}^*.$$

The corresponding theorem for $\int d\bar{\mu}$ (Theorem 3 SF) is less immediate. It can, however, be obtained rather more shortly than in SF by applying the following lemma (SF, 323) to $\bar{\boldsymbol{m}}$ upper measure.

LEMMA. *If $\boldsymbol{E}_1, \boldsymbol{E}_2, \cdots, \boldsymbol{E}_{2p}$ are mutually disjoint sets, then*

$$\sum_{n=1}^{P} \bar{\boldsymbol{m}}(\boldsymbol{E}_{2n-1} + \boldsymbol{E}_{2n}) - \bar{\boldsymbol{m}}(\sum_{i=1}^{2P} \boldsymbol{E}_i) \geq \sum_{n=1}^{P} \bar{\boldsymbol{m}}(\boldsymbol{E}_{2n}) - \bar{\boldsymbol{m}} \sum_{n=1}^{P} \boldsymbol{E}_{2n}.$$

We need consider only the case when the sets E_n are non-overlapping. Let $\boldsymbol{E}_{2n-1}$ denote the ordinate-set of f on E_n, and let $\boldsymbol{E}_{2n} = E_n \times J_0 - \boldsymbol{E}_{2n-1}$. The lemma then gives at once, for a finite sum of sets E_n,

$$\sum_{n=1}^{P} (M \cdot \bar{m} E_n - \int_{E_n} f \, d\bar{\mu}) - [M \cdot \bar{m}(\sum_{n=1}^{P} E_n) - \int_{\Sigma E_n} f \, d\bar{\mu}]$$
$$\leq M \cdot \sum_{n=1}^{P} \bar{m} E_n - M \cdot \bar{m}(\sum_{n=1}^{P} E_n);$$

that is,

$$\int_{\Sigma E_n} f \, d\bar{\mu} \leq \Sigma \int_{E_n} f \, d\bar{\mu}.$$

The passage to the limit to obtain the corresponding result when we have an infinite sequence of sets E_n is, in general, valid only when the upper measures $\bar{m}$ and $\boldsymbol{m}$ are regular—a case which we consider later.[17] The theorem is however always true if $\sum_{n=1}^{\infty} \bar{m} E_n$ is finite: for if we choose p so large that $\sum_{n=p+1}^{\infty} \bar{m} E_n < \epsilon$ (say), then $\bar{m}(\sum_{n=p+1}^{\infty} E_n) < \epsilon$ and so

$$\int_{\sum_{n=1}^{\infty} E_n} f \, d\bar{\mu} \leq \int_{\sum_{n=1}^{P} E_n} f \, d\bar{\mu} + \int_{\sum_{n=p+1}^{\infty} E_n} f \, d\bar{\mu} \leq \sum_{n=1}^{P} \int_{E_n} f \, d\bar{\mu} + M\epsilon,$$

from which the result follows.

---

[17] The following example shows that the theorem may fail for an infinite sequence of sets. Let E_0 consist of two infinite sequences of points (A_n) and (B_n). Let $m(E) = 2$ if E contains an infinite number of points A_n, and $m(E) = 1$ for all other non-empty sets, the empty set of course having zero measure. Let $f(x) = 1$ at each point A_n and $f(x) = 0$ at each point B_n, and let E_n consist of the two points A_n and B_n. It is easily verified that m satisfies conditions (a), (b) and (c), and that $\int_{E_n} f \, d\mu = 0$ for each n, while $\int_{\sum_{n=1}^{\infty} E_n} f \, d\mu = 1$.

6. We now consider Theorem 6 SF, or rather the equivalent theorem

$$\int (f+g)\,d\bar{\mu}^* \leq \int f\,d\bar{\mu}^* + \int g\,d\bar{\mu}^*.$$

This has an obvious similarity to the condition (b) satisfied by an upper-measure function, but it cannot be deduced simply by applying (b) to either $\overline{m \times L_1}$ or $\overline{m \times J_1}$ upper measure. It can, however, be expressed as a simple property of an upper measure $\overline{m \times J_1}^*$ which we now define.

Let $\boldsymbol{E}$ be any set in the (x, y) space, and, for given x, let $E(x)$ denote the set of y such that $(x, y) \epsilon \boldsymbol{E}$. Let (E_n) be any finite sequence of sets in the x-space, and denote by $c_n(x)$ the characteristic function of E_n. We shall say that *the sets E_n, associated with the heights l_n, form a skew covering of* $\boldsymbol{E}$ if, for each x, there exists in the y-space a set intervals I_n (depending on x) of respective lengths $l_n c_n(x)$, which cover $E(x)$. We define $\overline{m \times J_1}^*(\boldsymbol{E})$ as the lower bound of $\Sigma l_n \cdot \bar{m}(E_n)$ for all such finite skew coverings. It is at once clear that

$$\overline{m \times J_1}^*(\boldsymbol{E}) \leqq \overline{m \times J_1}(\boldsymbol{E})$$

and that

$$\overline{m \times J_1}^*(\boldsymbol{E}+\boldsymbol{E}') \leqq \overline{m \times J_1}^*(\boldsymbol{E}) + \overline{m \times J_1}^*(\boldsymbol{E}').[18]$$

THEOREM 4. *If $\boldsymbol{E}$ is the ordinate-set of f on E, then* $\overline{m \times J_1}^*(\boldsymbol{E}) = \overline{m \times J_1}(\boldsymbol{E}) = \int_E f\,d\bar{\mu}^*$.

Suppose given any skew covering of $\boldsymbol{E}$. By an arbitrarily small increase in the heights l_n we may suppose them all rational; let l be the largest number such that the numbers l_n/l are all integral. We may replace each set E_n, associated with l_n, by the set E_n repeated l_n/l times, associated each time with the height l. That is, it is sufficient to consider finite skew coverings $E_1, E_2, \cdots, E_p$ in which all the heights are the same, say l. We then have, clearly, $l\Sigma c_n(x) \geqq f(x)$ for all x of E. Now if $E_1 \supseteq E_2 \supseteq \cdots \supseteq E_p$, it is easily seen that the sets $E_1 \times \langle 0, l\rangle, E_2 \times \langle l, 2l\rangle, \cdots, E_n \times \langle (n-1)l, nl\rangle, \cdots$ form a finite covering of the ordinate-set of $f(x)$; that is, $\overline{m \times J_1}(\boldsymbol{E}) \leqq l\Sigma\bar{m}(E_n)$.

Suppose, however, that $E_1 \not\supset E_2$. Write $E'_1 = E_1 + E_2$, $E'_2 = E_1 E_2$, with characteristic functions c'_1 and c'_2 respectively. Then $c_1(x) + c_2(x) = c'_1(x) + c'(x)$ for all x, so that we may replace E_1, E_2 by E'_1, E'_2 and still have a skew covering of $\boldsymbol{E}$ with heights l. We now have $E'_1 \supset E'_2$ and $\bar{m}E'_1 + \bar{m}E'_2 \leqq \bar{m}E_1 + \bar{m}E_2$. If $E'_1 \not\supset E_3$ we can similarly replace E'_1, E_3

[18] We do not examine the question whether $\overline{m \times J_1}^*$ satisfies (b).

by $E'_1 + E_3$ and E'_1E_3 respectively: continuing this process, first with all pairs of integers $(1, i)$, then with all pairs $(2, i)$ such that $i > 2$, and so on, we finally obtain a skew covering by sets $E_1'', E_2'' \cdots$ (say), with heights l, such that $E_1'' \supset E_2'' \supset \cdots \supset E_p''$ and $\Sigma\bar{m}E_n'' \leqq \Sigma\bar{m}E_n$. Thus we have again

$$\overline{m \times J_1}(\boldsymbol{E}) \leqq l\Sigma\bar{m}E_n'' \leqq l\Sigma\bar{m}E_n.$$

We deduce at once that $\overline{m \times J_1}(\boldsymbol{E}) \leqq \overline{m \times J_1}^*(\boldsymbol{E})$ and therefore

$$\overline{m \times J_1}^*(\boldsymbol{E}) = \overline{m \times J_1}(\boldsymbol{E}).$$

Now consider two functions $f(x)$ and $g(x)$. Let $\boldsymbol{F}$ and $\boldsymbol{G}$ be the ordinate-sets of f and g on E, and $\boldsymbol{G}_1$ the set $f(x) < y \leqq f(x) + g(x)$, $x \in E$. Since, for any x, the sets $G(x)$ and $G_1(x)$ are congruent (except for a single point), any skew covering of $\boldsymbol{G}$ also provides a skew covering of $\boldsymbol{G}_1$, so that

$$\overline{m \times J_1}^*(\boldsymbol{G}) = \overline{m \times J_1}^*(\boldsymbol{G}_1).$$

We then have

$$\int_E (f + g)\,d\bar{\mu}^* = \overline{m \times J_1}^*(\boldsymbol{F} + \boldsymbol{G}_1) \leqq \overline{m \times J_1}^*(\boldsymbol{F}) + \overline{m \times J}^*(\boldsymbol{G}_1)$$
$$= \overline{m \times J_1}^*(\boldsymbol{F}) + \overline{m \times J_1}^*(\boldsymbol{G}) = \int_E f\,d\bar{\mu}^* + \int_E g\,d\bar{\mu}^*.$$

Suppose now that f is measurable $(\bar{m})$ relative to E, so that $\boldsymbol{F}$ is measurable $(\overline{m \times J_1})$ relative to $E \times J_0$. Then

$$\int_E (f + g)\,d\bar{\mu}^* = \overline{m \times J_1}(\boldsymbol{F} + \boldsymbol{G}_1) = \overline{m \times J_1}(\boldsymbol{F}) + \overline{m \times J_1}(\boldsymbol{G}_1)$$

(since $\boldsymbol{F}$ is measurable)

$$\geqq \overline{m \times J_1}(\boldsymbol{F}) + \overline{m \times J_1}^*(\boldsymbol{G}_1) = \int_E f\,d\bar{\mu}^* + \int_E g\,d\mu^*$$

as before. Theorem 5 SF follows at once.

7. From now on we supose that the upper measure $\bar{m}$ is regular. In this case the Fan integrals can be expressed in terms of integrals of the Lebesgue type, and some of the theorems of SF can thus be more easily proved. We also obtain some new theorems.

THEOREM 5. *If the upper measure $\bar{m}$ is regular, then the upper measure $\bar{\boldsymbol{m}}$ is regular, and the sets measurable $\bar{\boldsymbol{m}}$ coincide with the sets measurable* $(\overline{\mathcal{X}\mathcal{L}_1})$.

Let $\boldsymbol{E}$ be any set in the (x, y) space, and (ϵ_i) a sequence of positive numbers tending to zero. For each i there exists a sequence of sets $E_n{}^i \times J_n{}^i$, covering $\boldsymbol{E}$, such that $J_n{}^i$ is measurable $(\mathfrak{L}_1)$ and

$$\sum_n \bar{m}E_n{}^i \cdot | J_n{}^i | < \bar{\boldsymbol{m}}(\boldsymbol{E}) + \epsilon_i.$$

Let $H_n{}^i$ be an equimeasurable cover of $E_n{}^i$, for $\bar{m}$ upper measure. Then $\boldsymbol{H}^i = \sum_n (H_n{}^i \times J_n{}^i)$ is measurable $(\mathfrak{X}\mathfrak{L}_1)$ and satisfies

$$\bar{\boldsymbol{m}}(\boldsymbol{H}_i) \leq \sum_n \bar{m}H_n{}^i \cdot | J_n{}^i | < \bar{\boldsymbol{m}}(\boldsymbol{E}) + \epsilon_i.$$

Then $\boldsymbol{H} = \prod \boldsymbol{H}_i$ is measurable $(\mathfrak{X}\mathfrak{L}_1)$ and therefore certainly measurable $\bar{\boldsymbol{m}}$; it covers $\boldsymbol{E}$ and satisfies $\bar{\boldsymbol{m}}\boldsymbol{H} \leq \bar{\boldsymbol{m}}\boldsymbol{E}$.

If $\boldsymbol{E}$ is measurable $\bar{\boldsymbol{m}}$, we can find similarly a set measurable $(\mathfrak{X}\mathfrak{L}_1)$ covering $E_0 \times J_0 - \boldsymbol{E}$; that is, we can find a set $\boldsymbol{K}$, measurable $(\mathfrak{X}\mathfrak{L}_1)$ and contained in $\boldsymbol{E}$, such that $\bar{\boldsymbol{m}}\boldsymbol{K} = \bar{\boldsymbol{m}}\boldsymbol{E} = \bar{\boldsymbol{m}}\boldsymbol{H}$. $\boldsymbol{E} - \boldsymbol{K}$ is then a subset of $\boldsymbol{H} - \boldsymbol{K}$, which is measurable $(\mathfrak{X}\mathfrak{L}_1)$ and of zero measure; hence $\boldsymbol{E}$ is measurable $(\overline{\mathfrak{X}\mathfrak{L}}_1)$.

Now suppose that $\boldsymbol{E}$ is the ordinate-set of a function $f(x)$ on a set E. We can then, as in Theorem 2, take for the sets $E_n{}^i \times J_n{}^i$ the sets $E(f > y_n{}^i) \times \langle y_n{}^i, y_{n+1}{}^i \rangle$, together with $E \times (y = 0)$, where $0 = y_0{}^i < y_1{}^i \cdots < y_{N_i}{}^i = M$ is a suitable division of J_0. Since $E_{n+1}{}^i \subset E_n{}^i \subset E$ we may suppose that $H_{n+1}{}^i \subset H_n{}^i \subset H$, for all i and n, where H is a fixed equimeasurable cover of E. Then $\boldsymbol{H}^i$ is the ordinate-set of a function $F_i(x)$ defined on H and measurable $\bar{m}$, and $\boldsymbol{H}$ is the ordinate-set of the function $F(x) = \underline{\text{bound}}\, F_i(x)$, which is again measurable $\bar{m}$ and defined on H. Since $\boldsymbol{H}$ covers $\boldsymbol{E}$ and $\bar{\boldsymbol{m}}(\boldsymbol{H}) = \bar{\boldsymbol{m}}(\boldsymbol{E})$, we have $F(x) > f(x)$ for x in E, and

$$\text{(10)} \qquad \int_H F(x)\, d\bar{m} = \int_H F(x)\, d\bar{\mu}^* = \int_{E_1} F(x)\, d\bar{\mu}^* = \int_{E_1} f(x)\, d\bar{\mu}^*,$$

where the first integral is of Lebesgue type, constructed by the use only of measurable sets.

The function $F(x)$ is not uniquely determined, as there is a certain arbitrariness in the choice of ϵ_i, $y_n{}^i$ and $H_n{}^i$. However, as we shall now show, any two determinations of $F(x)$ differ only on a set of zero $\bar{m}$-measure.

THEOREM 6. (i) *If $G(x)$ is measurable $\bar{m}$ and $G(x) \geq f(x)$ on E, then $G(x) \geq F(x)$ almost everywhere $(\bar{m})$ on H.*[19]

[19] That is, except for a set of zero $\bar{m}$-measure. We note that a function measurable m and defined everywhere on E must be defined almost everywhere (m) on the equimeasurable cover, H, of E.

(ii) *For any* $\epsilon > 0$, $\bar{m}[E(f > F - \epsilon)] = \bar{m}E$.

(iii) *If* $F_1(x)$ *is measurable* $\bar{m}$, $F_1(x) \geq f(x)$ *on* E, *and, for any* $\epsilon > 0$, $\bar{m}[E(f > F_1 - \epsilon)] = \bar{m}E$, *then* $F_1(x) = F(x)$ *almost everywhere* $(\bar{m})$ *on* H.[19]

(iv) *For any* y, $\bar{m}[H(F > y)] = \bar{m}[E(F > y)] = \bar{m}[E(f > y)]$.

Proof. (i) Suppose that, if possible, $\bar{m}[H(G < F)] > 0$. For sufficiently small $\epsilon > 0$, we have $\bar{m}[H(G < F - \epsilon)] > 0$. The function $F_1(x) = \min[F(x), G(x)]$ is measurable $\bar{m}$ and $F_1(x) \geq f(x)$ on E. The ordinate-set of $F_1(x)$ on H includes the ordinate-set of $f(x)$ on E and so

$$\int_H F_1(x)\,d\bar{m} = \int_H F_1(x)\,d\bar{\mu}^* \geq \int_{E_1} f(x)\,d\bar{\mu}^*. \tag{11}$$

On the other hand, $F_1(x) \leq F(x)$ everywhere and $\bar{m}[H(F_1 < F - \epsilon)]$ is positive, say equal to η. Hence

$$\int_H F_1(x)\,d\bar{m} \leq \int_H F(x)\,d\bar{m} - \epsilon\eta. \tag{12}$$

Combining (10), (11) and (12) we have a contradiction.

As a corollary we see that if $F_1(x)$ is any other determination of $F(x)$, we have, almost everywhere $(\bar{m})$ on H, $F_1(x) \geq F(x)$ and $F(x) \geq F_1(x)$; that is, $F_1(x) = F(x)$.

We may say that $F(x)$ is effectively the smallest function, measurable $\bar{m}$, which is, everywhere on E, greater than or equal to $f(x)$. Accordingly we shall call it the *approximate maximal function of* $f(x)$ *on* E, and denote it by $A^*(f, E, \bar{m}; x)$, or simply $A^*(f)$ or $A^*(x)$ when there is no risk of confusion.[20]

(ii). Let E_ϵ denote $E(f > F - \epsilon)$, and let H_ϵ be an equimeasurable cover of E_ϵ; we may suppose $H_\epsilon \subset H$. If $\bar{m}E_\epsilon < \bar{m}E$, then $\bar{m}(H - H_\epsilon) > 0$. Writing $G(x) = F(x)$ on H_ϵ and $G(x) = F(x) - \epsilon$ on $H - H_\epsilon$, we obtain a contradiction with (i).

(iii). By (i), $\bar{m}[H(F_1 < F)] = 0$. For any $\epsilon > 0$, we have $\bar{m}[H(F > F_1 - \epsilon)] \geq \bar{m}[E(f > F_1 - \epsilon)] = \bar{m}E$, and so, since F and F_1 are measurable, $\bar{m}[H(F \leq F_1 - \epsilon)] = 0$. As ϵ is arbitrary, this gives $\bar{m}[H(F < F_1)] = 0$.

(iv). If, for any y_0, $\bar{m}[H(F > y_0)] > \bar{m}[E(f > y_0)]$, then there exists an $\epsilon > 0$ such that $\bar{m}[H(F > y_0 + \epsilon)] - \bar{m}[E(f > y_0)] = \alpha > 0$, say, since

---

[20] Cf. A. J. Ward, "On the differential structure of real functions," *Proceedings of the London Mathematical Society*, (2), vol. 39 (1935), pp. 339-362 (especially 341), where a rather different treatment is given in the special case of Lebesgue measure.

$\bar{m}[H(F > y_0)] = \lim_{\epsilon \to +0} \bar{m}[H(F > y_0 + \epsilon)]$. Accordingly $\bar{m}[H(F > y)] - \bar{m}[E(f > y)] \geq \alpha$ for $y_0 \leq y \leq y_0 + \epsilon$. It follows that

$$\int_0^M \bar{m}[H(F > y)]dy - \int_0^M \bar{m}[E(f > y)]dy$$
$$\geq \int_{y_0}^{y_0+\epsilon} \bar{m}[H(F > y)] - \bar{m}[E(f > y)]dy \geq \alpha\epsilon,$$

which contradicts (10).

It is clear that we could have defined the function $F(x) = A^*(f, E, \bar{m}; x)$ without any reference to $\bar{m}$ measure.[21] It is not difficult to prove Theorem 6 directly from such a definition without using our previous work. The equalities (10) then follow at once from Theorem 6, (iv). The remaining theorems of this paper might therefore have been proved independently of **1-6**.

We can construct in a corresponding way the approximate minimal function $A_*(f, E, \bar{m}; x)$ such that $\int_E f\, d\bar{\mu} = \int_H A_* d\bar{m}$. If $f(x)$ is integrable $(\bar{\mu})$ on E, we then have

$$\int_H A_* d\bar{m} = \int_E f\, d\bar{\mu} = \int_E f\, d\bar{\mu}^* = \int_H A^* d\bar{m}.\text{[22]} \tag{13}$$

Now $A^* \geq f \geq A_*$ on E, so that $\bar{m}[H(A^* \geq A_*)] \geq \bar{m}E = \bar{m}H$; accordingly, since A^* and A_* are measurable, $\bar{m}[H(A^* < A_*)] = 0$. It now follows from (13) that $A^* = A_*$ almost everywhere on H, and so $f = A^*$ almost everywhere on E. We thus find again the theorem [23] that if f is relatively measurable on E, then there exists a measurable function which coincides with f on E.

8. We can now give very simple proofs of Theorems 3 SF, 6 SF and 18 SF, using the standard properties of integrals of measurable functions. Let us consider first Theorem 3 SF. For each n, denote by H_n an equimeasurable cover of E_n; then $H = \Sigma H_n$ is an equimeasurable cover of $E = \Sigma E_n$. Let $F(x) = A_*(f, E; x)$, defined on H, and $F_n(x) = A_*(f, E_n; x)$, defined on H_n. Since $F(x)$ is measurable and $F(x) \leq f(x)$ on E_n, we have $F(x) \leq F_n(x)$ almost everywhere on H_n, as in Theorem 6 (i). Since $F(x)$ is non-negative and the sets H_n are measurable, but may overlap, we have

---

[21] From now on we use only m-measure: the words 'measurable' and 'almost everywhere' always refer to this measure.

[22] If K is an equimeasurable kernel of E (that is, $K \subset E$ and $\bar{m}K = \underline{m}K = \underline{m}E$), it follows from **1** that $\int_E f\, d\mu = \int_K A^*(f, K)dm$ and $\int_E f\, d\mu^* = \int_K A_*(f, K)dm$.

[23] J. C. Burkill and U. S. Haslam-Jones, "Relative measurability and the derivates of non-measurable functions," *Quarterly Journal of Mathematics* (Oxford), vol. 4 (1933), pp. 233-239, Theorem 7.

$$\int_H F(x)\,d\bar{m} \leq \Sigma \int_{H_n} F(x)\,d\bar{m} \leq \Sigma \int_{H_n} F_n(x)\,d\bar{m};$$

that is,

$$\int_E f(x)\,d\bar{\mu} \leq \Sigma \int_{E_n} f(x)\,d\bar{\mu}.$$

This applies whether the number of sets E_n is finite or enumerable.

To prove Theorem 6 SF, let $F(x) = A_*(f, E; x)$ and $G(x) = A_*(g, E; x)$. Then $F(x) + G(x)$ is measurable and $F(x) + G(x) \leq f(x) + g(x)$ on E; hence $F(x) + G(x) \leq A^*(f + g, E; x)$ almost everywhere on H. Accordingly we have

$$\int_E f\,d\bar{\mu} + \int_E g\,d\bar{\mu} = \int_H F\,d\bar{m} + \int_H G\,d\bar{m} = \int_H (F + G)\,d\bar{m}$$
$$\leq \int_H A_*(f + g, E; x)\,d\bar{m} = \int_E (f + g)\,d\bar{\mu}.$$

To prove Theorem 18 SF we have, similarly, $A_*(f_n, E; x) \leq f_n(x)$ on E, and so $\overline{\lim_{n\to\infty}}\, A_*(f_n, E; x) \leq \overline{\lim_{n\to\infty}}\, f_n(x)$. The function on the left is measurable and so $\overline{\lim_{n\to\infty}}\, A_*(f_n, E; x) \leq A_*(\overline{\lim_{n\to\infty}}\, f_n, E; x)$, almost everywhere on H. The result now follows by integration.

9. We now state two new theorems on the Fan integral.

THEOREM 7. *Given any set E (on which $f(x) \geq 0$) and any $\epsilon > 0$, there exists a set $S = S(\epsilon) \subset E$ such that*

$$\int_S f\,d\bar{\mu}^* = \int_E f\,d\bar{\mu}^*$$

and

$$\int_S f\,d\bar{\mu} \geq \int_S f\,d\bar{\mu}^* - \epsilon.$$

Let $F(x) = A^*(f, E, x)$ and let S_ϵ be the set on which $f(x) \geq F(x) - [\epsilon/\bar{m}E]$. Since $\bar{m}S = \bar{m}E = \bar{m}H$ we have by a remark in **1**,

$$\int_S f\,d\bar{\mu} \geq \int_S [F(x) - \epsilon/\bar{m}E]\,d\bar{\mu} \geq \int_H [F(x) - \epsilon/\bar{m}E]\,d\bar{\mu}$$
$$= \int_H [F(x) - \epsilon/\bar{m}E]\,d\bar{m} = \int_E f\,d\bar{\mu}^* - \epsilon.$$

For any $\eta < \epsilon$, $E \supset S_\epsilon \supset S_\eta$. Accordingly

$$\int_E f\,d\bar{\mu}^* \geq \int_{S_\epsilon} f\,d\bar{\mu}^* \geq \int_{S_\eta} f\,d\mu^* \geq \int_{S_\eta} f\,d\bar{\mu} \geq \int_E f\,d\bar{\mu}^* - \eta,$$

as above. Since η is arbitrary, $\int_{S_\epsilon} f\,d\bar{\mu}^* = \int_E f\,d\bar{\mu}^*$.

THEOREM 8.[24] *A necessary and sufficient condition that* $\int_E (f+g)\,d\bar{\mu}^* = \int_E f\,d\bar{\mu}^* + \int_E g\,d\bar{\mu}^*$ *(both functions being non-negative), is that, given any* $\epsilon > 0$, *there exists a set* $S = S_\epsilon \subset E$ *such that* $\bar{m}S = \bar{m}E$, $\int_S f\,d\bar{\mu} \geq \int_E f\,d\bar{\mu}^* - \epsilon$, *and* $\int_S g\,d\bar{\mu}^* = \int_E g\,d\bar{\mu}^*$.

(i) *Sufficiency.* If, for any $\epsilon > 0$, such a set S_ϵ exists, we have

$$\int_E (f+g)\,d\bar{\mu}^* \geq \int_{S_\epsilon} (f+g)\,d\bar{\mu}^* \geqq \int_{S_\epsilon} f\,d\bar{\mu} + \int_{S_\epsilon} g\,d\bar{\mu}^* \text{ (Theorem 9 SF)},$$

and since ϵ is arbitrary the result follows at once.

(ii) *Necessity.* We have, almost everywhere on H, $A^*(f+g) \leq A^*(f) + A^*(g)$ (the corresponding result for A_* has been proved in **8**). If

$$\int_E (f+g)\,d\bar{\mu}^* = \int_E f\,d\bar{\mu}^* + \int_E g\,d\bar{\mu}^*,$$

then

$$\int_H A^*(f+g)\,d\bar{m} = \int_H A^*(f)\,d\bar{m} + \int_H A^*(g)\,d\bar{m},$$

so that $A^*(f+g) = A^*(f) + A^*(g)$ almost everywhere on H. Let $S = S_\epsilon$ be the set on which $f + g > A^*(f+g) - (\epsilon/\bar{m}E)$ and also $A^*(f+g) = A^*(f) + A^*(g)$; then $\bar{m}S_\epsilon = \bar{m}E$. Since $A^*f \geqq f$ and $A^*g \geqq g$ on E, we must have, on S, $f > A^*(f) - (\epsilon/\bar{m}E)$ and $g > A^*(g) - (\epsilon/\bar{m}E)$. Just as in Theorem 7, we deduce that

$$\int_S f\,d\bar{\mu}^* = \int_E f\,d\bar{\mu}^*; \quad \int_S f\,d\bar{\mu} > \int_E f\,d\bar{\mu}^* - \epsilon,$$

with similar results for g at the same time.

VICTORIA UNIVERSITY,
MANCHESTER, ENGLAND.

[24] It is easily shown by an example that the ϵ cannot, in general, be omitted; it is not always possible to find $S \subset E$, with $\bar{m}S \subset \bar{m}E$, on which f is integrable $(\bar{\mu})$ and $\int_S g\,d\bar{\mu}^* = \int_E g\,d\bar{\mu}^*$. A similar remark applies to Theorem 7.

ξ^*

en

$\bar{\mu}$

),

)
If

N_e
)
C,
st

is
d